EXHIBIT L

Plaintiff's '619 Patent

US010984619B2

(12) **United States Patent**
Golden

(10) **Patent No.: US 10,984,619 B2**
(45) **Date of Patent: *Apr. 20, 2021**

(54) **MULTI SENSOR DETECTION, STALL TO STOP, AND LOCK DISABLING SYSTEM**

(71) Applicant: **Golden Larry**, Greenville, SC (US)

(72) Inventor: **Larry Golden**, Greenville, SC (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **16/350,683**

(22) Filed: **Dec. 19, 2018**

(65) **Prior Publication Data**

US 2019/0130679 A1 May 2, 2019

Related U.S. Application Data

(60) Continuation of application No. 15/530,839, filed on Mar. 6, 2017, now Pat. No. 10,163,287, which is a (Continued)

(51) **Int. Cl.**
G07C 9/00 (2020.01)
B60R 25/04 (2013.01)
(Continued)

(52) **U.S. Cl.**
CPC ***G07C 9/00563*** (2013.01); ***B60R 25/01*** (2013.01); ***B60R 25/04*** (2013.01);
(Continued)

(58) **Field of Classification Search**
CPC G07C 9/00; G07C 9/0007; G07C 9/00174; G07C 9/00309; G07C 9/00388;
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,385,469 A 5/1983 Scheuerpflug et al.
4,544,267 A 10/1985 Schiller
(Continued)

OTHER PUBLICATIONS

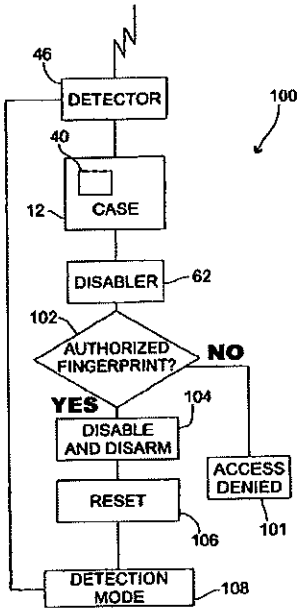
United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/199,853; copyright dated Jan. 13, 2012, pp. 1-34, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (34 pages).
(Continued)

Primary Examiner — Van T Trieu

(57) **ABSTRACT**

A multi sensor detection and disabling lock system includes detector cases for holding interchangeable detectors that sample for chemical, biological and radiological compounds, agents and elements, with each detector case disposed in or upon the monitored product. The detector case transmits detection information to a monitoring computer terminal and transmits a signal to a lock disabler engaged to the product to lock or disable the product's lock thereby preventing untrained, unauthorized and unequipped individuals from gaining access and entry to the product, and also preventing further contamination of the area. The detection system can be interconnected to surveillance towers scanning detector cases disposed at seaport docks, freight depots and rail terminals for monitoring containers being prepared for shipment or sitting on docks for long periods of time.

20 Claims, 13 Drawing Sheets



Related U.S. Application Data

continuation of application No. 14/806,988, filed on Jul. 23, 2015, now Pat. No. 9,589,439, which is a continuation of application No. 14/021,693, filed on Sep. 9, 2013, now Pat. No. 9,096,189, which is a continuation of application No. 13/288,065, filed on Nov. 3, 2011, now Pat. No. 8,531,280, which is a division of application No. 12/802,001, filed on May 27, 2010, now Pat. No. 8,334,761, which is a continuation of application No. 12/657,356, filed on Jan. 20, 2010, now Pat. No. 8,106,752, which is a continuation of application No. 12/155,573, filed on Jun. 6, 2008, now Pat. No. 7,636,033, which is a continuation-in-part of application No. 11/397,118, filed on Apr. 5, 2006, now Pat. No. 7,385,497.

(51) **Int. Cl.**

B60R 25/01	(2013.01)
B60R 25/102	(2013.01)
G08B 13/24	(2006.01)
B60R 25/104	(2013.01)
G08B 25/00	(2006.01)
H04W 4/80	(2018.01)
G07C 9/20	(2020.01)
G08B 15/00	(2006.01)
G08B 21/12	(2006.01)
B60R 25/24	(2013.01)

(52) **U.S. Cl.**

CPC ***B60R 25/102*** (2013.01); ***G08B 13/2491*** (2013.01); *B60R 25/018* (2013.01); *B60R 25/104* (2013.01); *B60R 25/24* (2013.01); *G07C 9/00174* (2013.01); *G07C 9/00912* (2013.01); *G07C 9/20* (2020.01); *G08B 15/00* (2013.01); *G08B 21/12* (2013.01); *G08B 25/009* (2013.01); *H04W 4/80* (2018.02)

(58) **Field of Classification Search**

CPC .. G07C 9/00563; G08B 27/00; G08B 27/005; G08B 27/006; G08B 15/00; G08B 15/001; G08B 15/004; G08B 15/009; B60R 25/018; B60R 25/04; B60R 25/10; B60R 25/102; B60R 25/0405; B60R 25/104

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,586,441	A	5/1986	Zekich	
4,792,226	A	12/1988	Fishbine et al.	
5,222,152	A	6/1993	Fishbine et al.	
5,223,844	A	6/1993	Mansell et al.	
5,233,404	A	8/1993	Lougheed et al.	
5,557,254	A	9/1996	Johnson et al.	
5,682,133	A	10/1997	Johnson et al.	
5,766,956	A	6/1998	Groger et al.	
5,938,706	A	8/1999	Feldman	
5,959,529	A	9/1999	Kail	
5,963,657	A	10/1999	Bowker et al.	
5,986,543	A	11/1999	Johnson	
5,990,785	A	11/1999	Suda	
6,049,269	A	4/2000	Byrd et al.	
6,078,265	A	6/2000	Bonder et al.	
6,236,365	B1 *	5/2001	LeBlanc	G01C 21/206 342/457
6,262,656	B1	7/2001	Byrd et al.	
6,271,745	B1	8/2001	Anzai et al.	
6,374,652	B1	4/2002	Hwang	
6,411,887	B1	6/2002	Martens et al.	
6,470,260	B2	10/2002	Martens et al.	
6,542,076	B1	4/2003	Joao	
6,542,077	B2	4/2003	Joao	
6,588,635	B2	7/2003	Vor Keller et al.	
6,610,977	B2	8/2003	Megerle	
6,613,571	B2	9/2003	Cordery et al.	
6,628,813	B2	9/2003	Scott et al.	
6,647,328	B2	10/2003	Walker	
6,738,697	B2	5/2004	Breed	
6,923,509	B1	8/2005	Barnett	
6,980,092	B2	12/2005	Turnbull et al.	
6,988,026	B2	1/2006	Breed et al.	
7,005,982	B1	2/2006	Frank	
7,034,677	B2	4/2006	Steinthal et al.	
7,034,683	B2	4/2006	Ghazarian	
7,103,460	B1	9/2006	Breed	
7,116,798	B1	10/2006	Chawla	
7,148,484	B2	12/2006	Craig et al.	
7,164,117	B2	1/2007	Breed et al.	
7,171,312	B2	1/2007	Steinthal et al.	
7,243,945	B2	6/2007	Breed et al.	
7,339,469	B2	3/2008	Braun	
7,346,439	B2	3/2008	Bodin	
7,350,608	B2	4/2008	Fernandez	
7,385,497	B2	6/2008	Golden	
7,397,363	B2	7/2008	Joao	
7,636,033	B2	12/2009	Golden	
7,647,180	B2	1/2010	Breed	
7,844,505	B1	11/2010	Arneson et al.	
7,868,912	B2	1/2011	Venetianer et al.	
7,872,575	B2	1/2011	Tabe	
7,880,767	B2	2/2011	Chinigo	
7,961,094	B2	6/2011	Breed	
8,120,459	B2	2/2012	Kwak	
8,274,377	B2	9/2012	Smith et al.	
8,531,521	B2	9/2013	Romanowich	
8,564,661	B2	10/2013	Lipton et al.	
8,615,290	B2	12/2013	Lin et al.	
2002/0145666	A1	10/2002	Scaman	
2003/0063004	A1	4/2003	Anthony et al.	
2003/0093187	A1 *	5/2003	Walker	B64C 13/20 701/1
2003/0137426	A1	7/2003	Anthony et al.	
2003/0179073	A1	9/2003	Ghazarian	
2003/0206102	A1	11/2003	Joao	
2004/0107028	A1	6/2004	Catalano	
2004/0222092	A1	11/2004	Musho	
2005/0195069	A1	9/2005	Dunand	
2006/0164239	A1	7/2006	Loda	
2006/0176169	A1	8/2006	Doolin et al.	
2006/0181413	A1	8/2006	Mostov	
2006/0250235	A1	11/2006	Astrin	
2006/0261931	A1 *	11/2006	Cheng	B60R 25/102 340/426.1
2007/0093200	A1	4/2007	Dobosz	
2007/0171042	A1	7/2007	Metes et al.	
2007/0257774	A1	11/2007	Stumpert et al.	
2008/0045156	A1	2/2008	Sakhpara	
2008/0122595	A1	5/2008	Yamamichi et al.	
2008/0234907	A1	9/2008	Labuhn et al.	
2009/0289780	A1 *	11/2009	Tenorio-Fox	B60R 25/04 340/425.5
2010/0159983	A1	5/2010	Golden	
2010/0265068	A1 *	10/2010	Brackmann	B60P 3/14 340/572.1
2011/0178655	A1	6/2011	Golden	

OTHER PUBLICATIONS

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/065,837; copyright dated Dec. 2, 2011, pp. 1-27, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (27 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/065,837; copyright dated Nov. 1, 2011, pp. 1-18, publisher United States Patent and Trademark

(56) **References Cited**

OTHER PUBLICATIONS

Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (18 pages).
United States Patent and Trademark Office; Office Action from U.S. Appl. No. 11/397,118; dated Nov. 14, 2007; Alexandria, Virginia, USA; pp. 1-12; U.S. Appl. No. 13/288,065 (12 pages).
United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/155,573; dated Apr. 9, 2009; Alexandria, Virginia, USA; pp. 1-7; U.S. Appl. No. 13/288,065 (7 pages).
United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/155,573; dated Jul. 30, 2009; Alexandria, Virginia, USA; pp. 1-9; U.S. Appl. No. 13/288,065 (9 pages).
United States Patent and Trademark Office; Notice of Allowability from U.S. Appl. No. 12/155,573; dated Oct. 28, 2009; Alexandria, Virginia, USA; pp. 1-5; U.S. Appl. No. 13/288,065 (5 pages).
United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/657,356; dated Jul. 12, 2010; Alexandria, Virginia, USA; pp. 1-14; U.S. Appl. No. 13/288,065 (14 pages).
United States Patent and Trademark Office; Notice of Allowability from U.S. Appl. No. 12/657,356; dated Mar. 10, 2011; Alexandria, Virginia, USA; pp. 1-4; U.S. Appl. No. 13/288,065 (4 pages).
United States Patent and Trademark Office; Office Action from U.S. Appl. No. 13/065,837; dated Jul. 18, 2011; Alexandria, Virginia, USA, pp. 1-9; U.S. Appl. No. 13/288,065 (9 pages).
A newspaper article of Mr. Melvin Sullivan and his family that references the date, Mar. 6, 2001. U.S. Appl. No. 13/288,065.
A letter of response Mr. Sullivan received from Pfeiffer & Gantt, PA, dated Sep. 16, 2002. U.S. Appl. No. 13/288,065.
A "Certificate of Existance" Bright Idea Inventor, LLC. Nov. 6, 2002. U.S. Appl. No. 13/288,065.
A letter of response Golden received from the Honorable Congressman from Maryland, Elijah E. Cummings, dated Dec. 16, 2002; U.S. Appl. No. 13/288,065.
A newspaper article of Mr. Melvin Sullivan and Mr. Larry Golden, dated, Feb. 27-Mar. 5, 2003; U.S. Appl. No. 13/288,065.
A letter of response Golden received from the Honorable Senator from South Carolina, Ernest F. Hollings, dated May 21, 2003; U.S. Appl. No. 13/288,065.
A letter of response Golden received from the Office of the Vice President, Dick Cheney, dated Jun. 3, 2003; U.S. Appl. No. 13/288,065.
A letter of response Golden received from the Honorable Senator from South Carolina, Ernest F. Hollings, dated Oct. 1, 2003; U.S. Appl. No. 13/288,065.
A letter of response Golden received from the Honorable Senator from South Carolina, Lindsey O. Graham, dated Oct. 21, 2003; U.S. Appl. No. 13/288,065.
A letter sent to the President of the United States George W Bush, the President's Cabinet, the United States Senate and the Congressional Black Caucus, dated May 23, 2005; U.S. Appl. No. 13/288,065.
On Nov. 17, 2005, an "Inventor's Official Record of Invention", was filed in my name (Golden) at "The Law Office of David P. Gaudio, P.C.; the Inventors Network."; U.S. Appl. No. 13/288,065.
On Aug. 23, 2005, the "Disclosure Document Registration"; U.S. Appl. No. 13/288,065.
On Apr. 5, 2006, the "Patent Application" was filed in my name (Golden) at the United Staets Patent & Trademark Office in Washington, D.C.; U.S. Appl. No. 13/288,065.
On Jun. 6, 2008, the "Continuance-In-Part, (CIP) Application" was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.; U.S. Appl. No. 13/288,065.
On Jan. 20, 2010, a "Continuation Application" (U.S. Appl. No. 12/657,356) was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.; U.S. Appl. No. 13/288,065.
Reissue of U.S. Pat. No. 7,636,033;"Swear Back"; in accordance to Title 37—Code of Federal Regulations Patents, Trademarks, and Copyrights; Apr. 8, 2011; U.S. Appl. No. 13/288,065.
Reissue of U.S. Pat. No. 7,636,033; "Swearback—History of Work"; Apr. 8, 2011; U.S. Appl. No. 13/288,065.
United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001; dated Apr. 14, 2011, 2011; Alexandria, Virginia, USA; pp. 1-16; U.S. Appl. No. 13/288,065 (16 pages).
United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001; dated May 27, 2011; Alexandria, Virginia, USA; pp. 1-14; U.S. Appl. No. 13/288,065 (14 pages).
United States Department of Homeland Security; Petition for Inter Partes Review of U.S. Pat. No. Re. 43,990 Under 35 U.S.C. §312 and 37 C.F.R. §42.104; Case IPR2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr. 30, 2014; Washington, D.C., USA; pp. 1-57, U.S. Appl. No. 14/806,988 (57 pages).
United States Department of Homeland Security; Declaration of Dr. Sriram Vishwanath; Case IPR2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr. 30, 2014; Washington, D.C., USA; pp. 1-44; U.S. Appl. No. 14/806,988 (44 pages).
Richard R Brooks and S.S. Iyengar; Multi-Sensor Fusion Fundamentals and Applications with Software; published 1998; Copyright Prentice Hall PTR; Upper Saddle River, New Jersey, USA; pp. 1-20; (20 pages). U.S. Appl. No. 14/806,988 (20 pages).
Ramanarayanan Viswanathan and Pramod K Varshney; Distriubted Detection with Multiple Sensors: Part I—Fundamentals; Proceedings of the IEEE; Jan. 1, 1997; pp. 1-11; vol. 85; No. 1; Southern Illinois University Carbondale OpenSIUC; Illinois, USA; pp. 1-11; U.S. Appl. No. 14/806,988 (11 pages).
Blum; Distributed Detection with Multiple Sensors: Part II—Advanced Topics; Proceedings of the IEEE; Jan. 1, 1997; pp. 1-16; vol. 85, No. 1; Southern Illinois University Carbondale OpenSIUC; Illinois, USA; U.S. Appl. No. 14/806,988 (16 pages).
Victor Lesser; Distributed Sensor Networks a Multiagent Perspective; 2003; pp. 1, 2, 5, 6, 22, 26, 27, 36, 275, 320; copyright 2003 Kluwer Academic Publishers; AH Dordrecht, The Netherlands; U.S. Appl. No. 14/806,988 (10 pages).
Samuel Blackman and Robert Popoli; Design and Analysis of Modern Tracking Systems; 1999; pp. 1, 2, 6, 472; copyright 1999 Artech House; Norwood, Massachusetts, USA; U.S. Appl. No. 14/806,988 (4 pages).
Jean-Francois Chamberland; Decentralized Detection in Sensor Networks; 2003; pp. 407-416; IEEE Transactions on Signal Processing; vol. 51, No. 2; Urbana, Illinois, USA; U.S. Appl. No. 14/806,988 (10 pages).
Oleg Kachirski and Ratan Guha; Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks; pp. 1-8; Proceedings of the 36.sup.th Hawaii International Conference on System Sciences; copyright 2003; Orlando, Florida, USA; U.S. Appl. No. 14/806,988 (8 pages).
Lawrence A Klein; Sensor and Data Fusion A Tool for Information Assessment and Decision Making; 2004; pp. 1-4, 6, 81, 87-89; copyright 2004 The Society of Photo-Optical Instrumentation Engineers; Publisher is SPIE—the International Society for Optical Engineering; Bellingham, Washington, USA; U.S. Appl. No. 14/806,988 (12 pages).
Dale Ferriere and Khrystyna Pysareva and Andrzej Rucinski; Using Technology to Bridge Maritime Security Gaps; Aug. 1, 2005; Sea Technology; pp. 1-6; copyright Compass Publications, Inc. Jan. 2009; Portsmouth, New Hampshire, USA; U.S. Appl. No. 14/806,988 (6 pages).
Corie Lok; Cargo Security; MIT Technology Review; Jun. 2004; No. 107; pp. 74-75; publisher is Massachusetts Institute of Technology; Cambridge, Massachusetts, USA; U.S. Appl. No. 14/806,988 (2 pages).
Thomas C Chen; RFID and Sensor-based Container Content Visibility and Seaport Security Monitoring system; Proceedings of SPIE, vol. 5778; pp. 151-159; Mar. 28, 2005; Publisher is SPIE—the International Society for Optical Engineering; Bellingham, Washington, USA; U.S. Appl. No. 14/806,988 (10 pages).
United States Department of Homeland Security; The University of Texas at Austin College of Engineering Standard Resume of Sriram Vishwanath; Case IPR2014-00714 for U.S. Pat. No. Re. 43,990; Filed Apr. 30, 2014; Washington, D.C., USA; pp. 1-21; U.S. Appl. No. 14/806,988 (21 pages).
Operating Agreement of Bright Idea Inventor, LLC received from Pfeiffer & Gantt, PA, dated Nov. 13, 2002; U.S. Appl. No. 13/288,065.

(56) **References Cited**

OTHER PUBLICATIONS

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001; dated Oct. 20, 2011; Alexandria, Virginia, USA; pp. 1-5; parent U.S. Appl. No. 13/288,065 (5 pages); U.S. Appl. No. 13/288,065 (5 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 12/802 001; copyright dated Dec. 12, 2011, pp. 1-9, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 13/288,065 (9 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 12/802,001; copyright dated Mar. 26, 2012, pp. 1-12, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (12 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/199,853; copyright dated Feb. 22, 2012, pp. 1-38, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (38 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/065,837; copyright dated Feb. 22, 2012, pp. 1-25, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (25 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright dated Aug. 24, 2012, pp. 1-4, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (4 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright dated Nov. 28, 2012, pp. 1-11, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (11 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 13/288,065; copyright dated Apr. 16, 2013, pp. 1-9, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 13/288,065 (9 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 14/021,693; copyright dated Apr. 20, 2015, pp. 1-20, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 14/021,693 (20 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 14/021,693; copyright dated Jan. 20, 2015, pp. 1-17, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 14/021,693 (17 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 14/021,693; copyright dated Sep. 5, 2014, pp. 1-12, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; U.S. Appl. No. 14/021,693 (12 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 14/806,988; copyright dated Jul. 5, 2015, pp. 1-5, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 14/806,988 (5 pages).

United States Patent and Trademark Office; Notice of Allowance from U.S. Appl. No. 14/806,988; dated Jan. 3, 2017; Alexandria, Virginia, USA; pp. 1-8; U.S. Appl. No. 14/806,988 (8 pages).

United States Patent and Trademark Office; Notice of Allowance from U.S. Appl. No. 14/021,693; dated Jun. 19, 2015; Alexandria, Virginia, USA; pp. 1-8; U.S. Appl. No. 14/021,693 (8 pages).

United States Patent and Trademark Office; Notice of Allowance from U.S. Appl. No. 13/288,065; dated May 24, 2013; Alexandria, Virginia, USA; pp. 1-8; U.S. Appl. No. 13/288,065 (8 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 15/530,839; copyright dated Sep. 26, 2018, pp. 1-9, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; parent U.S. Appl. No. 15/530,839 (9 pages).

United States Patent and Trademark Office; Notice of Allowance from U.S. Appl. No. 15/530,839; copyrighted dated May 16, 2018; Alexandria, Virginia, USA; pp. 1-7; U.S. Appl. No. 15/530,839 (7 pages).

Letter from Applicant, Larry Golden regarding Written Description dated Dec. 3, 2019.

Deignan, abstract,Wearable Chemical Sensors: Characterization of Heart Rate Electrodes Using Electrochemical Impedance Spectroscopy,12th Ann. BodySensor Network Con. Jun. 9-12, 2015.

My Tutor website, "How does the body increase heart rate in response to exercise?" https://www.mytutor.co.uk/answers/8802/A-Level/Biology, printed Dec. 3, 2019.

Portions of Moore, Jason, "HRV Demographics: Part 1—Age & Gender," HRVcourse.com, https://hrvcourse.com/hrv-demographics-age-gender/, copyright 2017, portion printed Dec. 2, 2019.

Hernandez, et al., abstract, "Wearable Motion-Based Heart Rate at Rest: A Workplace Evaluation," IEEE J BiomedHealth Inform, Sep. 2019; pp. 1920-1927.

Kalnoskas, A.,Biometric Sensors Include Advanced Heart Monitoring & ECG, Nov. 30, 2017, www.microcontrollertips.com/biometric-sensors-include-advanced-heart-monitoring-and-ecg/.

Holder, et al., pportions of "Using What You Get: Dynamic Physiologic Signatures of Critical Illness," Crit Care Clin, Jan. 2015: 31 (1): 133-164, p. 1 of 35

Brain Signs website,webpage entitled: "ElectroCardioGaphy(ECG) & Heart Rate (HR)," copyrighted 2018, printed Dec. 2, 2019, www.brainsigns.com/en/science/s2/technologies/hr.

Johnson,Carolyn Y., "Spotting a Terrorist," article, Boston Globe, pub. Sep. 18, 2009.

Letter, from applicant, Larry Golden, ATPG Technology, LLC, to Bruce Sewell, • SVP 7 General Counsel, Apple. Inc. dated Nov. 11, 2010.

* cited by examiner

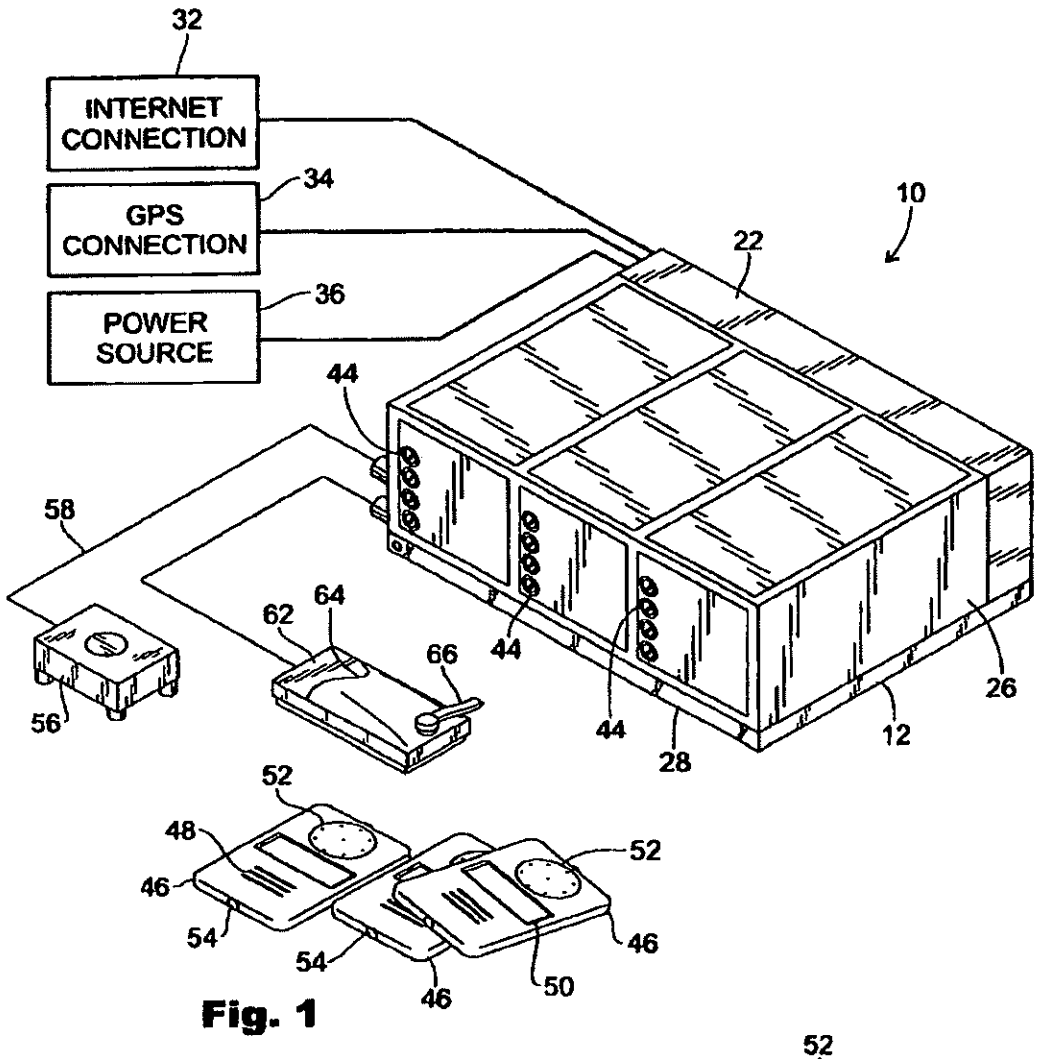

32
INTERNET CONNECTION
34
GPS CONNECTION
36
POWER SOURCE
10
22
44
58
62
64
66
56
44
28
12
26
52
48
46
54
54
46
52
46
50

Fig. 1

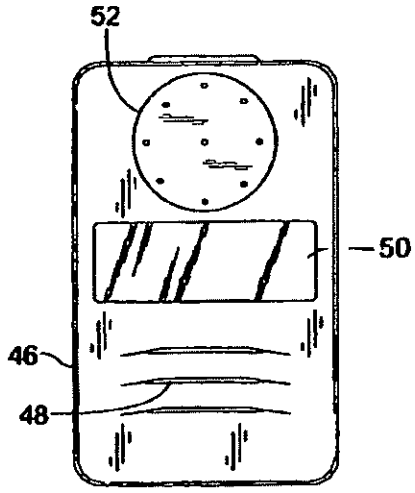

52
50
46
48

Fig. 2

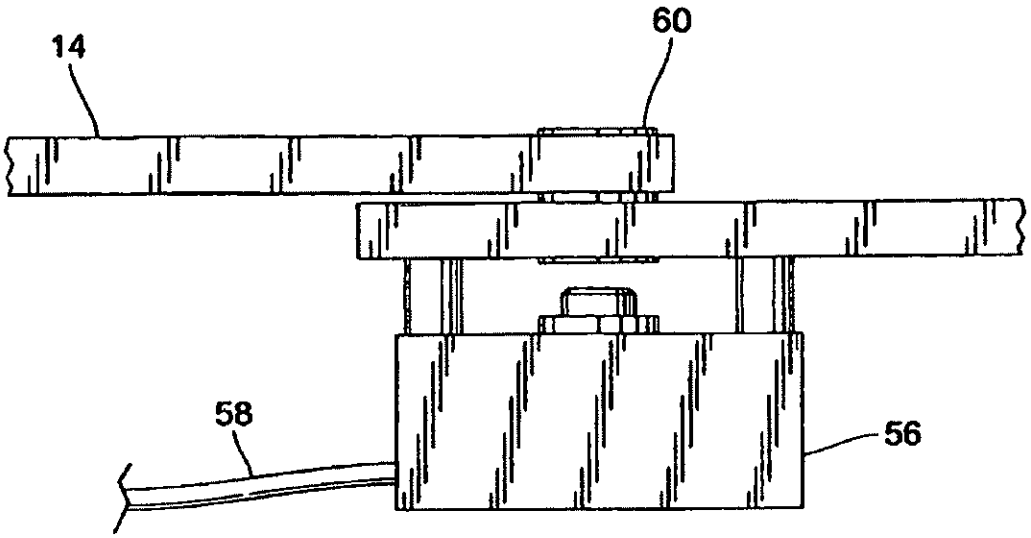


Fig. 3a

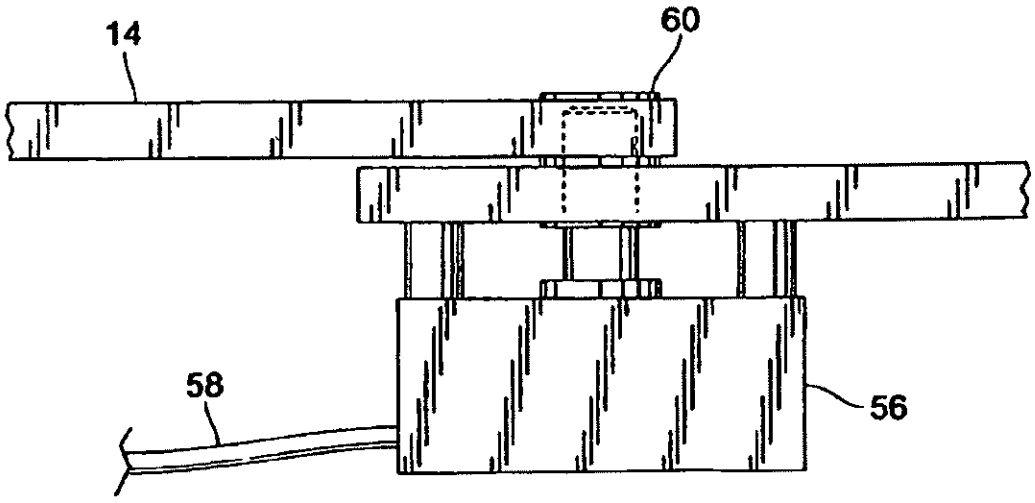


Fig. 3b

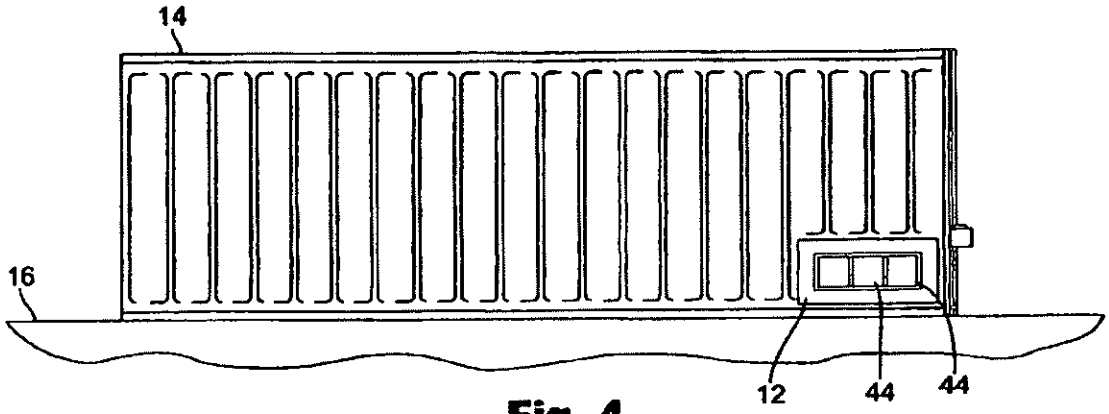


Fig. 4

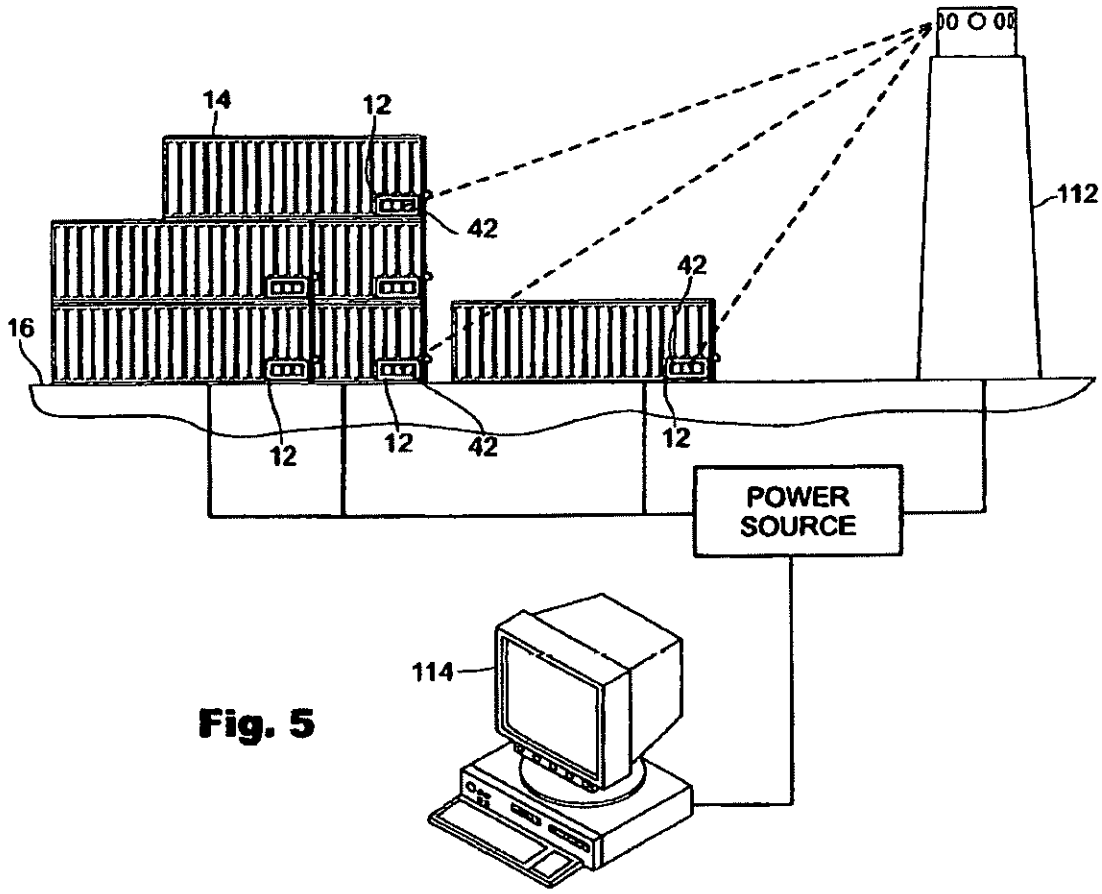


Fig. 5

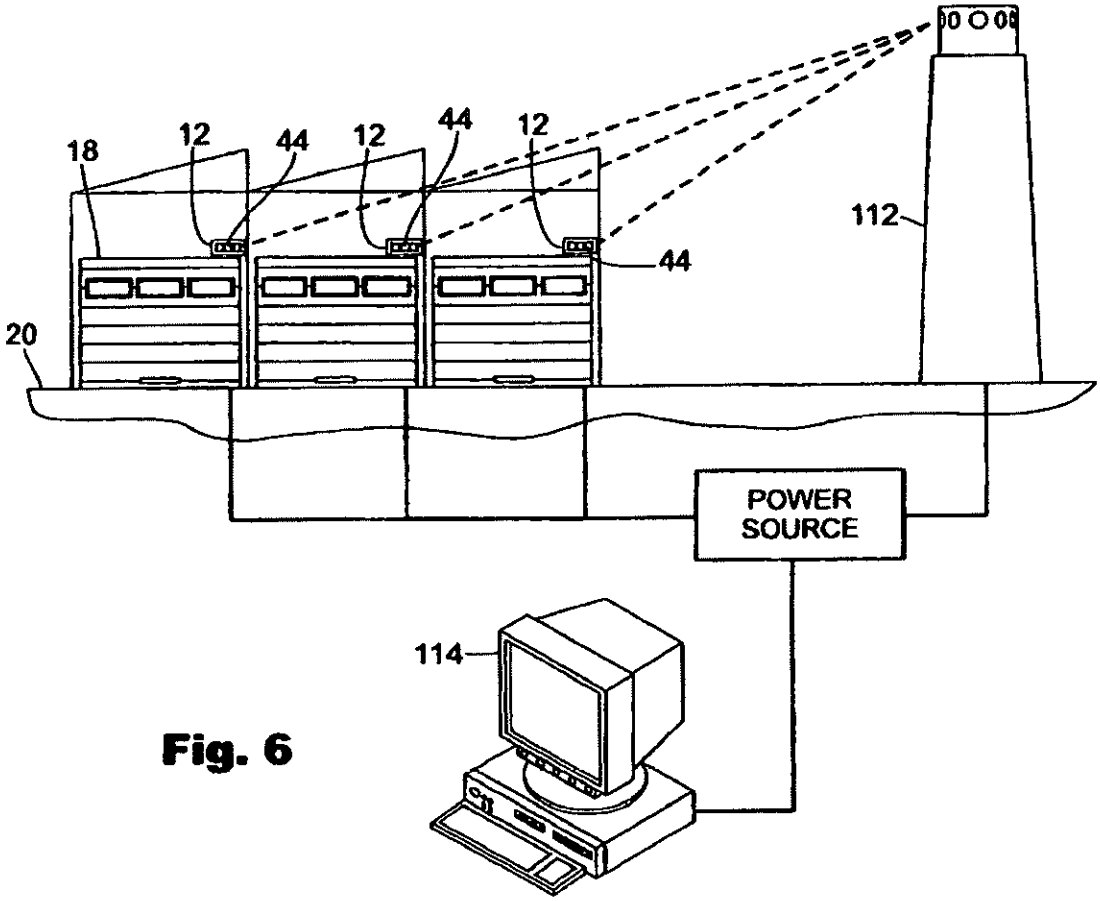


Fig. 6

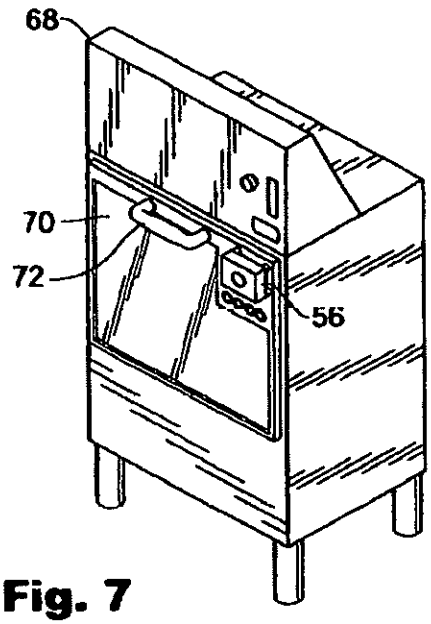


Fig. 7

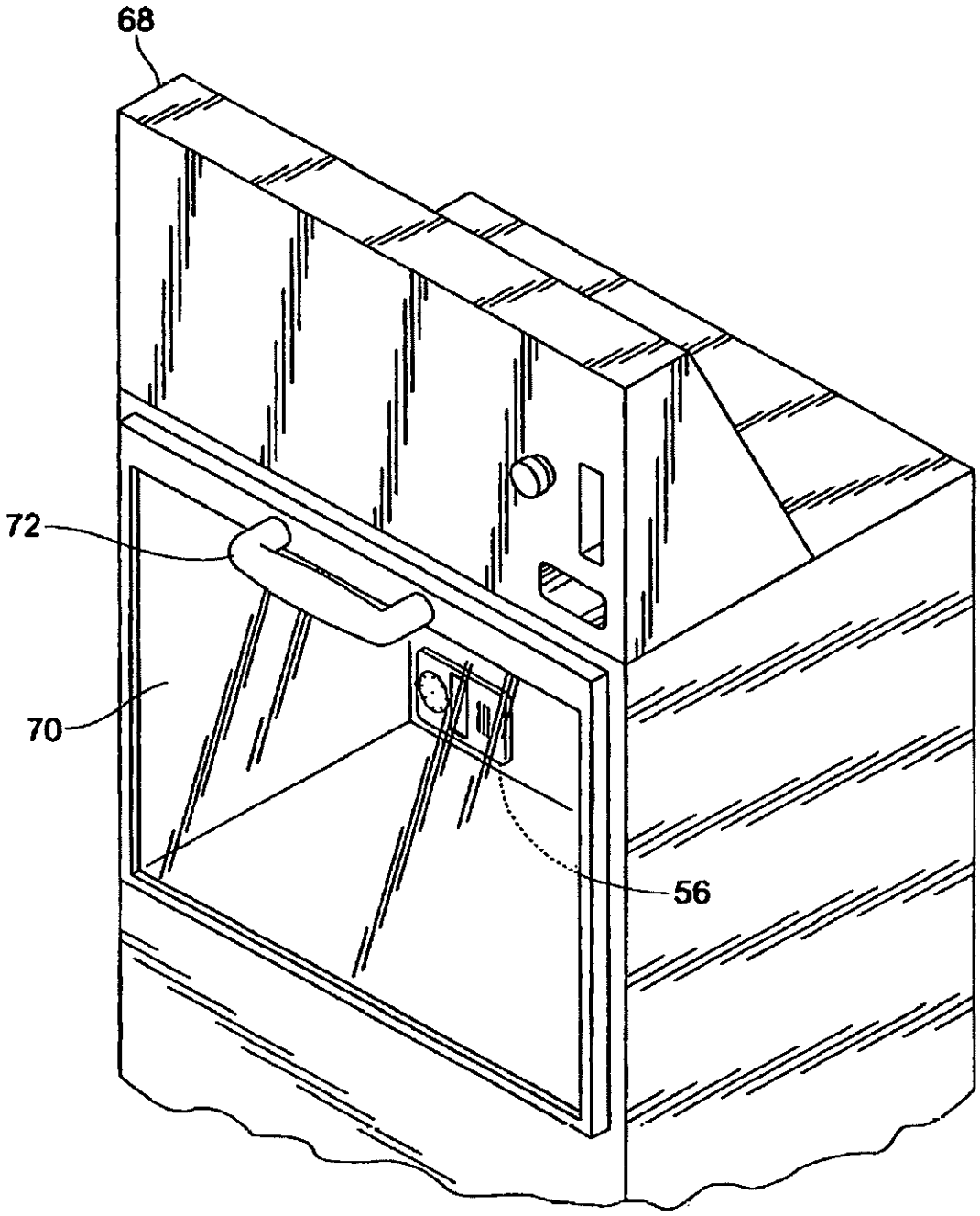


Fig. 8

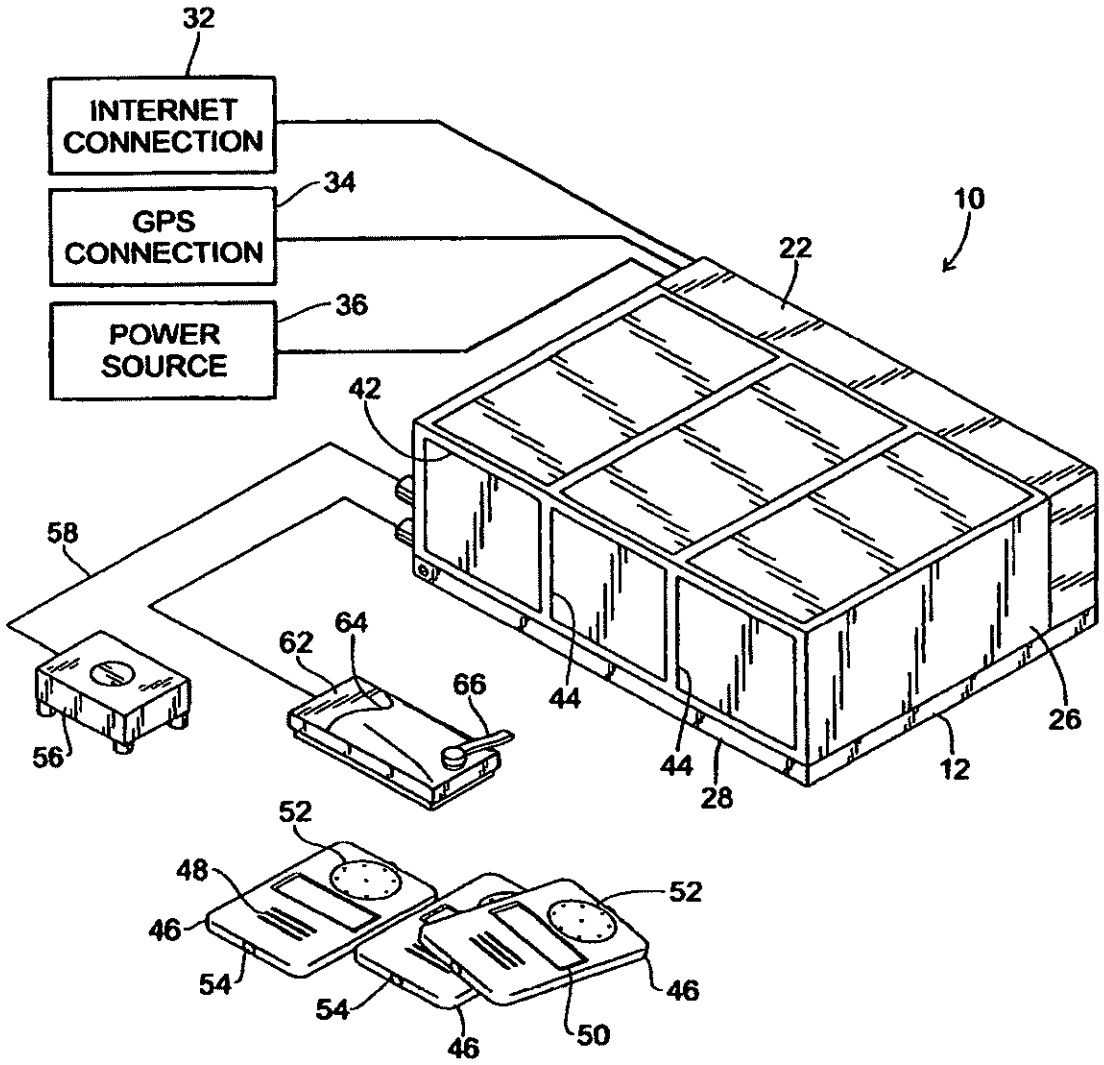

32
INTERNET CONNECTION
34
GPS CONNECTION
36
POWER SOURCE
10
22
42
58
62
64
66
44
44
28
12
26
56
52
48
46
54
54
46
50
52
46

Fig. 9

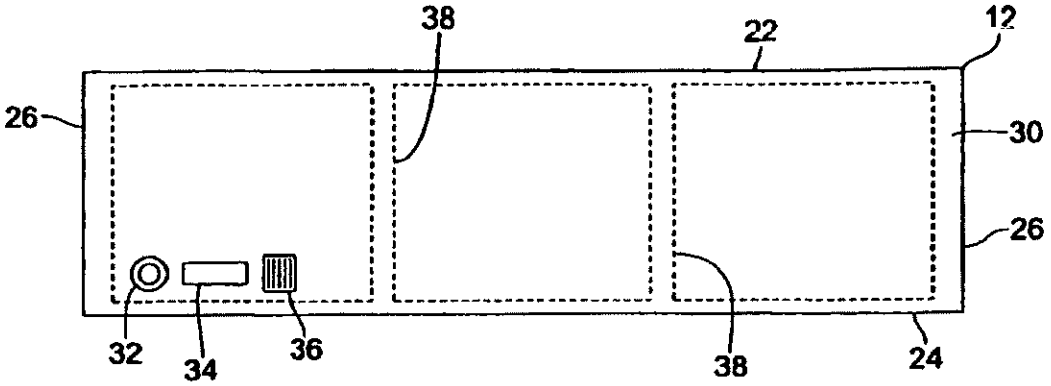

38
22
12
26
30
26
32
34
36
38
24

Fig. 10

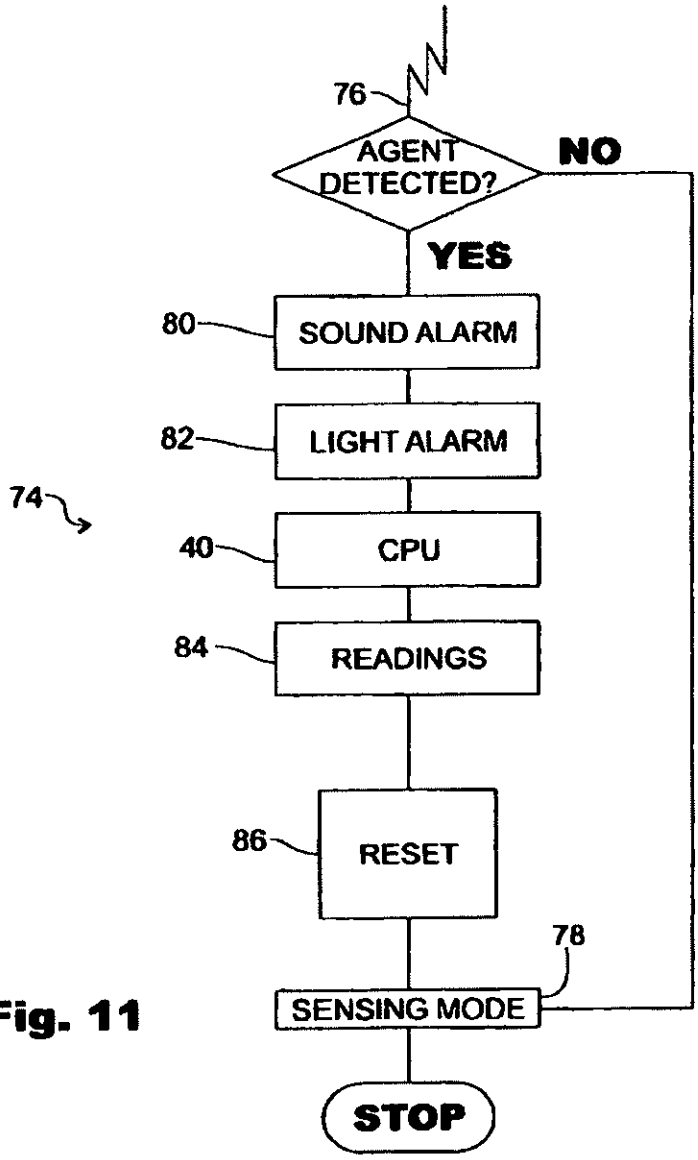

76
AGENT DETECTED?
NO
YES
80
SOUND ALARM
82
LIGHT ALARM
74
40
CPU
84
READINGS
86
RESET
78
SENSING MODE
STOP

Fig. 11

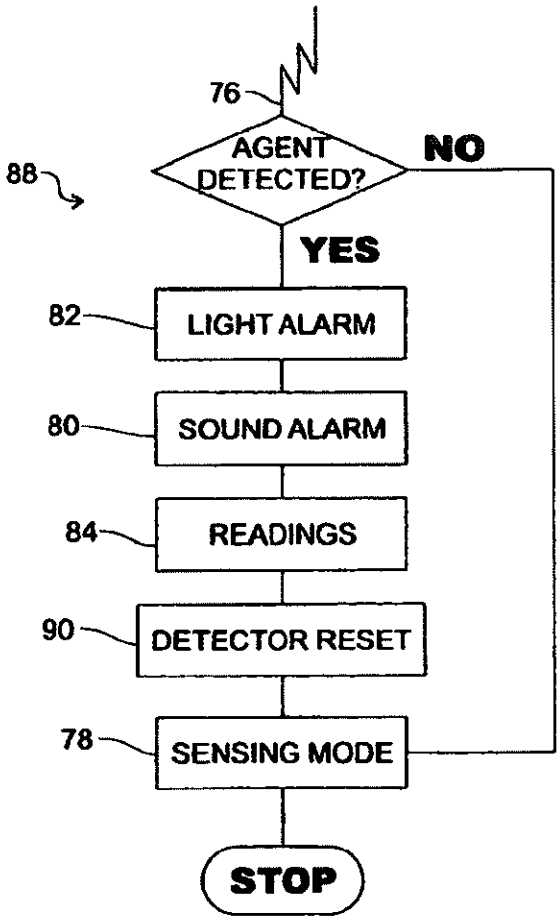

76
AGENT DETECTED?
NO
88
YES
82
LIGHT ALARM
80
SOUND ALARM
84
READINGS
90
DETECTOR RESET
78
SENSING MODE
STOP

Fig. 12

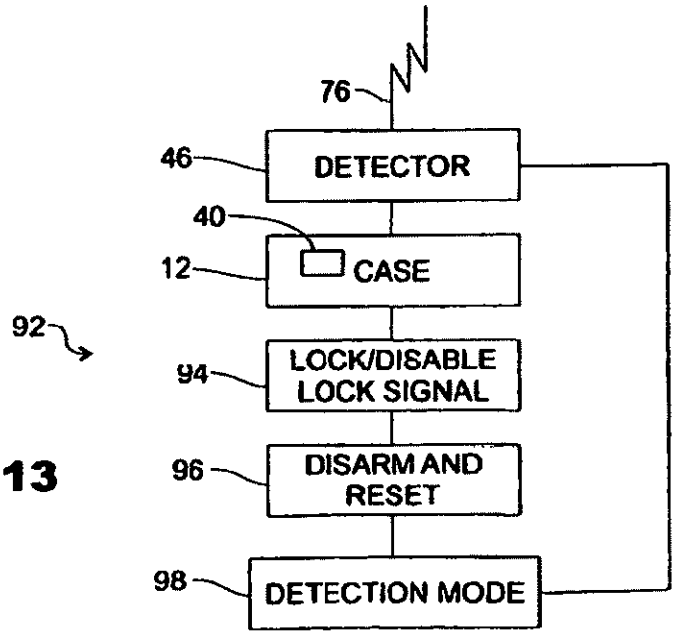

76
46
DETECTOR
40
12
CASE
92
94
LOCK/DISABLE LOCK SIGNAL
96
DISARM AND RESET
98
DETECTION MODE

Fig. 13

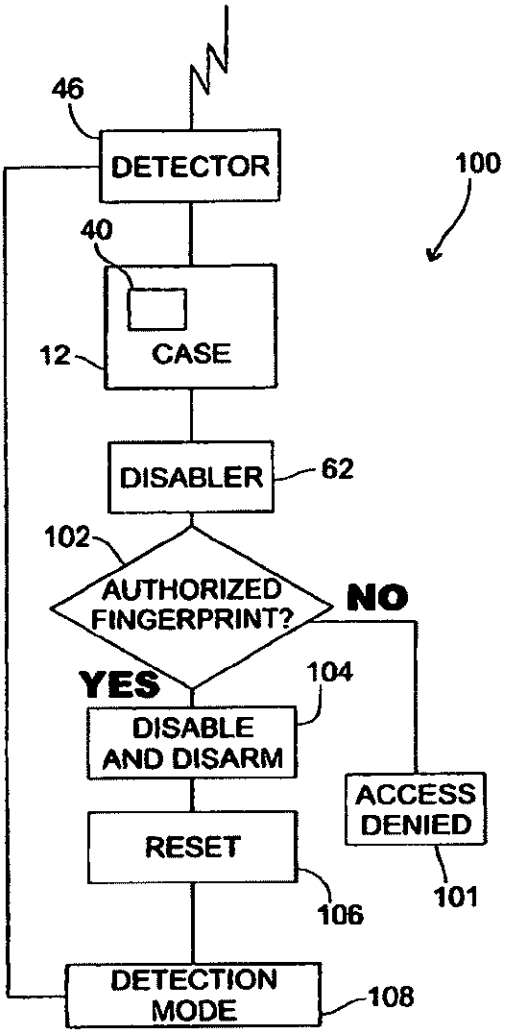

46
DETECTOR
100
40
CASE
12
DISABLER
62
102
AUTHORIZED FINGERPRINT?
NO
YES
104
DISABLE AND DISARM
ACCESS DENIED
101
RESET
106
DETECTION MODE
108

Fig. 14

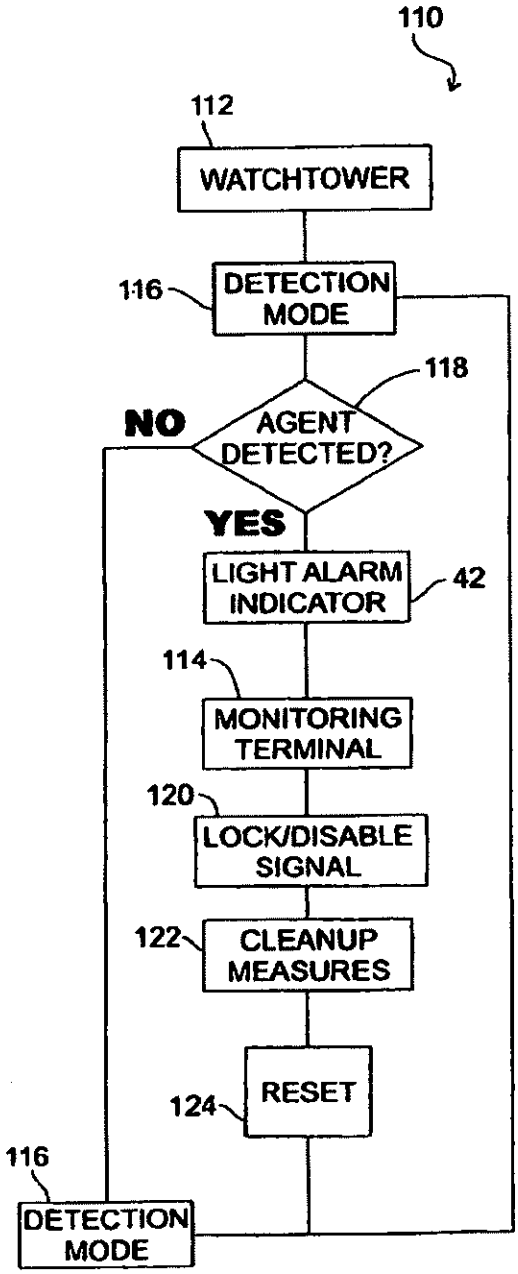

110
112
WATCHTOWER
116
DETECTION MODE
118
NO
AGENT DETECTED?
YES
LIGHT ALARM INDICATOR
42
114
MONITORING TERMINAL
120
LOCK/DISABLE SIGNAL
122
CLEANUP MEASURES
RESET
124
116
DETECTION MODE

Fig. 15

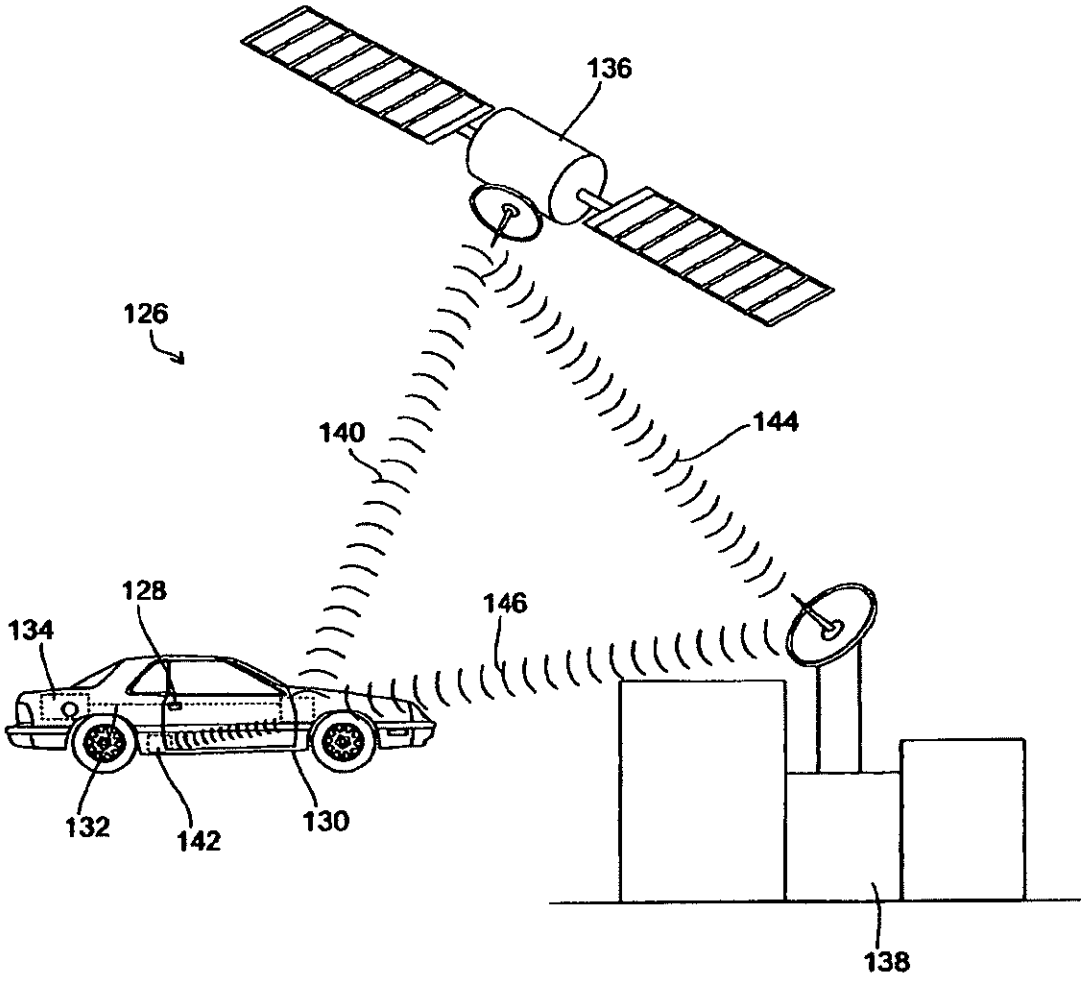


Fig. 16

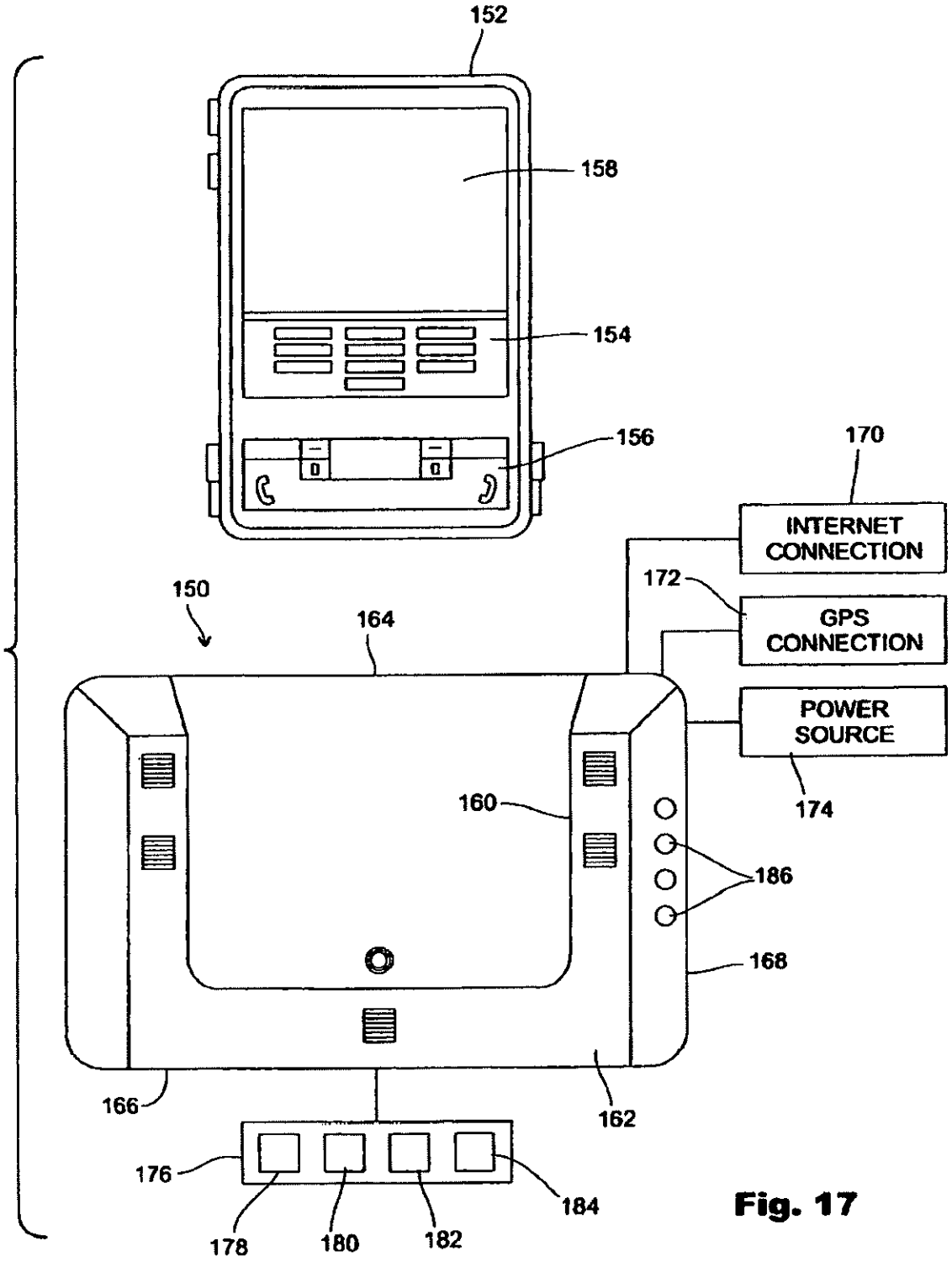

152
158
154
156
170
INTERNET CONNECTION
172
GPS CONNECTION
POWER SOURCE
174
150
164
160
186
168
166
162
176
178
180
182
184

Fig. 17

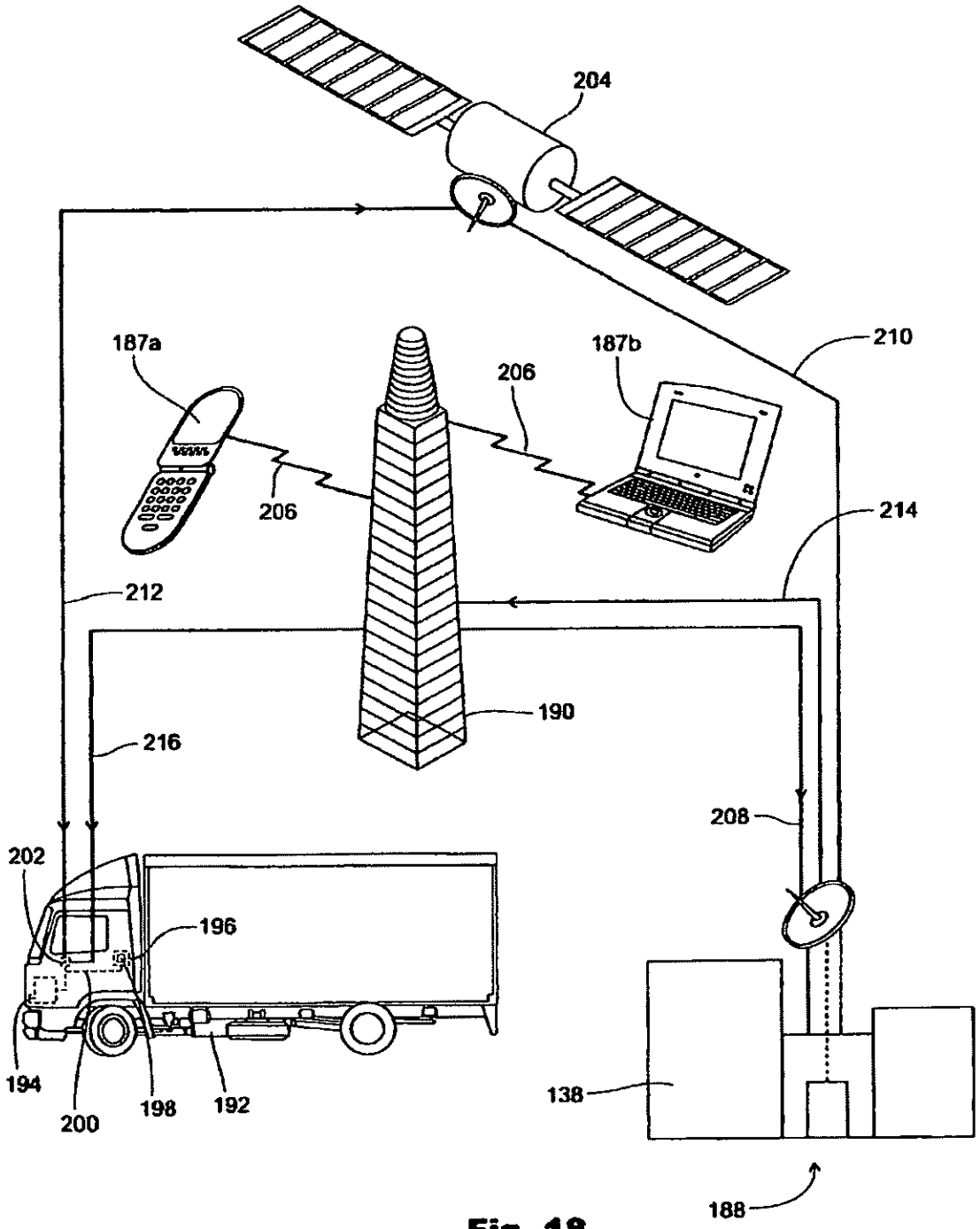

204
187a
187b
206
210
206
214
212
190
216
208
202
196
194
200
198
192
138
188

Fig. 18

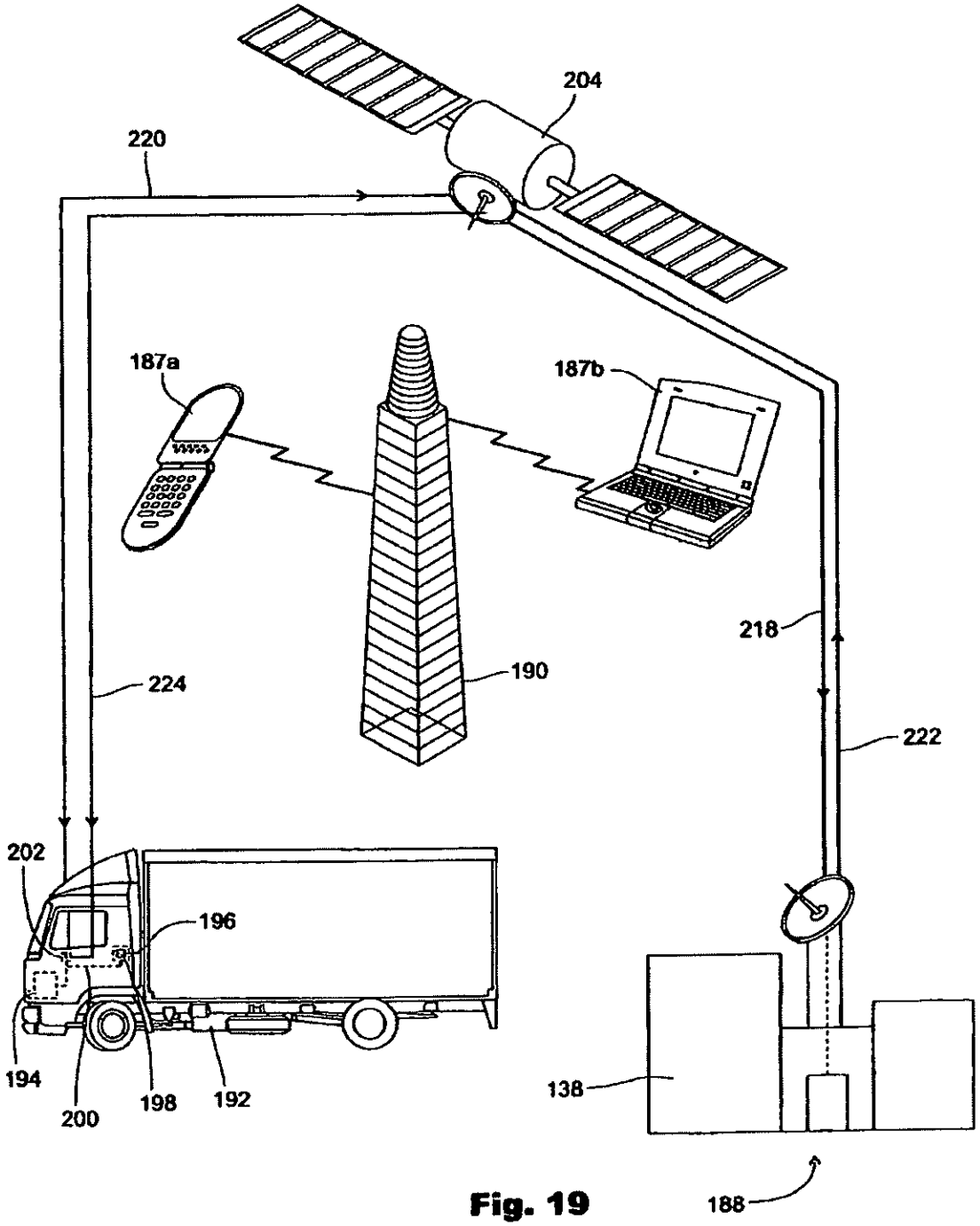

204
220
187a
187b
218
190
224
222
202
196
194
200
198
192
138
188

Fig. 19

MULTI SENSOR DETECTION, STALL TO STOP, AND LOCK DISABLING SYSTEM

CROSS REFERENCE TO RELATED APPLICATION

This application is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 15/530,839 titled "Multi Sensor Detection, Stall to Stop, and Lock Disabling System" filed on Mar. 6, 2017, the entire contents and complete subject matter of which is incorporated by reference herein in its entirety for all purposes. U.S. patent application Ser. No. 15/530,839 issued as U.S. Pat. No. 10,163,287, is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 14/806,988 filed on Jul. 23, 2015, issued as U.S. Pat. No. 9,589,439, and incorporates the entire contents and complete subject matter therein by reference in their entirety for all purposes. U.S. patent application Ser. No. 14/806,988 is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 14/021,693 filed on Sep. 9, 2013, issued as U.S. Pat. No. 9,096,189, and incorporates the entire contents and complete subject matter therein by reference in their entirety for all purposes. U.S. patent application Ser. No. 14/021,693 is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 13/288,065 filed on Nov. 3, 2011, issued as U.S. Pat. No. 8,531,280, and incorporates the entire contents and complete subject matter therein by reference in their entirety for all purposes. U.S. patent application Ser. No. 13/288,065 is a divisional application and claims the filing date and benefit of U.S. patent application Ser. No. 12/802,001 filed on May 27, 2010, issued as U.S. Pat. No. 8,334,761, and incorporates the entire contents and complete subject matter therein by reference in their entirety for all purposes. U.S. patent application Ser. No. 12/802,001 is a continuation application and claims the filing date and benefit of U.S. patent application Ser. No. 12/657,357 filed on Jan. 20, 2010, issued as U.S. Pat. No. 8,106,752, and incorporates the entire contents and complete subject matter therein by reference in their entirety for all purposes. The present application also claims the filing dates and benefits of and incorporates the entire contents of U.S. patent application Ser. Nos. 14/806,988; 14/021,693; 13/288,065; 12/802,001; 12/657,356, 12/155,573, issued as U.S. Pat. No. 7,636,033, and Ser. No. 11/397,118, issued as U.S. Pat. No. 7,385,497, herein by reference for all purposes.

FIELD OF THE INVENTION

The present invention pertains to anti-terrorist detection and prevention systems, and more particularly pertains to a disabling lock mechanism combined with a chemical/biological/radiological detection system for use with products grouped together by similar characteristics in order to prevent unauthorized entry, contamination and terrorist activity.

BACKGROUND

Terrorist activity is a continuous, daily, worldwide threat to the stability, prosperity, security and peace within nations and between and among nations. Its danger lies in its arbitrary destructiveness as much as in its unpredictability, and the constant threat of terrorist activity compels measures and actions that cause strain and contention in free, democratic societies as security concerns and civil liberty concerns must be balanced so that both public safety and civil liberties are maintained. Safety and security concerns can be addressed through numerous proactive steps and measures, many of which cause only minimal interference with and disruption of the daily routines of work, travel, commerce and entertainment. However, because modern industrial societies afford almost limitless places, locations, and opportunities for terrorist activities, no safety measure or security protocol will be foolproof, but many security measures, systems and protocols can be implemented that greatly minimize specific threats through fingerprint identification procedures, chemical, biological, and radiological hazard detections, bomb and explosive detection, and controlling the access to everything from shipping containers to school lockers. Thus, the prior art discloses a wide range of security measures and systems.

For example, the Fishbine et al. patent (U.S. Pat. No. 4,792,226) discloses an optical fingerprinting system that includes an optics/processor unit, a video monitor, a data terminal, and a printer for collecting and storing data characteristics of all ten individual fingerprints for printing demographic information and fingerprint images as desired on a standard booking or applicant card.

The Schiller patent (U.S. Pat. No. 4,544,267) discloses a finger identification unit that includes a fingerprint scanning apparatus using a collimated beam of light to interrogate the fingerprint of a finger placed against a platen so that successive scan positions produce signals containing fingerprint information.

The Fishbine et al. patent (U.S. Pat. No. 5,222,152) discloses a portable fingerprint scanning apparatus for optically scanning and recording fingerprint images and wirelessly transmitting such images to a mobile processing unit for verification and background checking.

The Lougheed et al. patent (U.S. Pat. No. 5,233,404) discloses an optical scanning apparatus that uses a linear charge coupled device (CCD) for recording the image of a fingerprint on the viewing surface.

The Groger et al. patent (U.S. Pat. No. 5,766,956) discloses a diode laser based sensor for undertaking optical, chemical, immunological or nucleic acid-based assay or other chemical analysis.

The Feldman patent (U.S. Pat. No. 5,938,706) discloses a multi element security system for preventing the unauthorized use of an automotive vehicle, and which includes numerous locking and control features interconnected to an onboard cpu.

The Bowker et al. patent (U.S. Pat. No. 5,963,657) discloses a safety access control for doors, handles, locks, etc., wherein the surface relief of a finger is read and verified to either allow or prevent access by the individual to the door, handle, lock, etc.

The Bonder et al. patent (U.S. Pat. No. 6,078,265) discloses a fingerprint identification security system wherein a key lock operated security system utilizes the fingerprint of the individual to control user access to the security system, such as the ignition system of an automotive vehicle.

The Anzai et al. patent (U.S. Pat. No. 6,271,745 B1) discloses a keyless authorization system for use of a motor vehicle that includes fingerprint reading units located on the exterior or interior of the motor vehicle and which are coupled to a control unit for scanning, comparing and matching fingerprints to allow or disallow access to the motor vehicle.

The Hwang patent (U.S. Pat. No. 6,374,652 B1) discloses a fingerprint-activated doorknob in which a detecting sensor for a fingerprint is placed on the doorknob for measuring and

searching the fingerprint against previously stored fingerprint inputs to control access to the door.

The Vor Keller et al. patent (U.S. Pat. No. 6,588,635 B2) discloses a safety holster for a firearm that includes a pivotally mounted retaining member and a fingerprint sensor for scanning fingerprint information so that only authorized users can withdraw the firearm from the holster.

The Cordery et al. patent (U.S. Pat. No. 6,613,571 B2) discloses a method and system for detecting biological and chemical hazards in the mail that includes sensors placed within the mail box for sampling and testing ambient air and so that mail can be safely transported through the mail system.

The Nagata patent (U.S. Pat. No. 6,628,213 B2) discloses a coding method for digital signal coding and decoding that includes a CMI (code-marked inversion) method of signal coding.

Nonetheless, despite the ingenuity of the above devices, methods, and systems, there remains a need for a multi-detector and disabling lock system for use with various types of products collected together by common characteristics into product groupings for detecting chemical, biological and radiological agents and compounds and for selectively disabling and activating the product locks thereby preventing unauthorized entry and further contamination and preventing and thwarting terrorist activities.

SUMMARY

The present invention comprehends a chemical/biological/radiological detector unit with a disabling locking system for protecting products that can be grouped into several product groupings, from terrorist activity, and also for preventing unauthorized access to and tampering with the storage and transport of ordnance and weapons. The products grouped into what may be referred to as Product grouping 1 include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes and lockers; while the products grouped into what may be referred to as Product grouping 2 include, but are not limited to, chemical, biological, radiological, and nuclear detectors, motion sensors and door sensors. The multi sensor detection system includes the capability to disable an existing lock or activate a lock located inside any of the products named in the product grouping categories upon activation of a sensor or detector included in the system. This is a significant feature for the multi sensor detection system as it prevents unauthorized, unequipped and untrained entry and access to the product thus preventing further contamination of the site and to individuals in the area.

The multi sensor detection and lock disabling system includes a detector case sized to fit in, upon or adjacent any of the aforedescribed products for detecting harmful and dangerous chemical, biological, and radiological agents, compounds and elements. In addition, the multi sensor detection and lock disabling system is capable of transmitting a signal to lock or disable a lock on the product, and is also capable of transmitting signals to a monitoring computer terminal or PC so that appropriate defensive and safeguarding actions can be undertaken and an authorized individual can disarm and reset the locking system and the multi sensor detection system. The detector case includes a power source (battery or electrical), interior compartments, Internet and GPS connections and a cpu interconnected with the Internet and GPS connections, and also interconnected with one or more off site monitoring computer terminals or PCs. The detector case includes one or more light alarm indicators that are externally visible and that light up when the chemical, biological, or radiological agent or compound is detected, and the light alarm indicators (which can be indicator lights or panels on the front of the detector case) can be color coded for denoting the specific agent or compound detected, i.e., separate and distinct colors for indicating detection of the chemical, biological, or radiological agent or compound.

The detector case is designed to hold within the interior compartments one or more interchangeable detectors, and each detector is adapted and set up to sample a specific compound or agent. Each detector includes a sound alarm, a sensor, a light alarm, and a readings panel, and is electrically interconnected (either by wire or wirelessly) to the cpu of the detector case so that information regarding the detection of the particular agent or compound can be conveyed from the detectors to the detector case cpu. Each detector can also be used as a manual, stand-alone hand held scanner.

The multi sensor detection and lock disabling system can be interconnected to a surveillance watchtower, as well as monitoring computer terminals or PCs, with the watchtower scanning shipping and cargo crates and containers being prepared for shipment or sitting for extended periods of time on a dock or at a port, at a railway site, or at an industrial storage facility. The watchtower will scan the cargo and shipping crates and containers for the light alarm indicators on detector cases that are mounted in or upon the crates and containers, and thus continuous security surveillance of the crates and containers can be maintained.

An enhanced version of the multi sensor detection and lock disabling system can be employed to prevent car and vehicle bombings. Coupling the multi sensor detection and lock disabling system with satellite service will enable the detection system to detect explosives and transmit an alert signal by satellite to monitoring equipment at a monitoring site. Upon receiving the alert signal at the monitoring site the monitoring equipment activates a stall-to-stop process for disabling the air, fuel, electrical and/or computer system of the vehicle. Moreover, upon receiving the alert signal at the monitoring site the car or vehicle will be locked by transmission of a satellite signal that disables the vehicle's electrical and ignition system thereby preventing escape of the terrorist.

It is an objective of the present invention to provide a multi sensor detection and disabling lock system for securing news racks and vending machines in order to prevent theft, unauthorized use and terrorist activity.

It is another objective of the present invention to provide a multi sensor detection and disabling lock system for preventing terrorist activity by using products grouped together by common features in several product groupings such as design similarity, similarity in the presentation of security problems and similarity with regard to the presentation of solutions to preventing terrorist solutions.

It is still yet another objective of the present invention to provide a multi sensor detection and disabling lock system that is capable of disabling an existing lock or activating a lock inside any of the products of the product grouping lists when a detector or sensor of the system is activated.

It is still yet a further objective of the present invention to provide a multi sensor detection and disabling lock system wherein the disabling lock system prevents the unauthorized entry, access and further contamination of the products included in the several product groupings.

A still further objective of the present invention is to provide a multi sensor detection and lock disabling system that utilizes a multi-task device for preventing terrorist

activity to vulnerable products that are collected or arranged by product grouping categories.

Yet a further objective of the present invention is to provide a multi sensor detection and disabling lock system to secure cargos and containers, especially cargo and shipping containers, against chemical, biological, radiological and nuclear terrorist activity.

Still another objective of the present invention is to provide a multi sensor detection and disabling lock system capable of detecting chemical, biological and radiological agents and compounds.

Still yet another objective of the present invention is to provide a multi sensor detection and disabling lock system that includes interchangeable detectors that operate in conjunction to detect chemical, biological and radiological agents and compounds.

Still yet a further objective of the present invention is to provide a multi sensor detection and disabling lock system that can be implemented by business or government at a minimum cost by organizing the products to be protected into product grouping categories.

Another objective of the present invention is to provide a multi sensor detection and disabling lock system that accurately and reliably detects harmful agents, compounds and elements, and prevents the placement and storage of weapons and bombs in the range of storage containers and facilities currently available.

Still another objective of the present invention is to provide a multi sensor detection and disabling lock system wherein the interchangeable detectors that comprise part of the system can be used as stand-alone scanners.

These and other objects, features, and advantages will become apparent to those skilled in the art upon a perusal of the following detailed description read in conjunction with the accompanying drawing figures and appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the primary features of the system which include a detector case, several interchangeable detectors, an automatic/mechanical lock disabler and a fingerprint biometric lock with disabler;

FIG. **2** is a front elevational view of the multi sensor detection and lock disabling system of the present invention illustrating one of the interchangeable detectors first shown in FIG. **1**;

FIG. **3***a* is a top plan view of the multi sensor detection and lock disabling system of the present invention illustrating the mounting of one lock disabler to the lock of a product, such as a container, and disengaged from the lock of the container;

FIG. **3***b* is a top plan view of the multi sensor detection and lock disabling system of the present invention illustrating the engagement of the lock disabler to the lock of the product for locking or disabling the lock of the product so that unauthorized access is prevented;

FIG. **4** is a side elevational view of the multi sensor detection and lock disabling system of the present invention illustrating the detector case mounted to the product, such as the container, with the light alarm indicators externally visible;

FIG. **5** is a schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of detector cases with a surveillance watchtower and a monitoring PC terminal;

FIG. **6** is a schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the placement of detector cases upon containers different from the containers of FIG. **5**, and wherein the detectors case are interconnected to a surveillance watchtower and a monitoring PC terminal;

FIG. **7** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the mounting of one automatic/mechanical lock disabler to the lock of a standalone news rack;

FIG. **8** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating one interchangeable detector placed within the standalone news rack;

FIG. **9** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the detector case having color coded front panels for specifically indicating the agents, compounds or elements that have been detected;

FIG. **10** is a rear elevational view of the multi sensor detection and lock disabling system of the present invention illustrating the GPS, Internet and power source connections;

FIG. **11** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of the detector with the detector case and the steps undertaken by the system when an agent or compound is detected;

FIG. **12** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the sequence of steps undertaken by one detector when functioning as a stand-alone scanner for detecting an agent or compound;

FIG. **13** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of the detector case with the automatic/mechanical lock disabler for activating the lock disabler upon detection by the system of an agent or compound;

FIG. **14** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating interconnection of the detector case with the fingerprint biometric lock with disabler for engaging and disengaging the fingerprint biometric lock as part of the process of detection and safeguarding the public upon detection of the agent or compound;

FIG. **15** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of the system with a surveillance watchtower and a monitoring PC or computer terminal for monitoring containers, such as shipping or cargo containers, that may sit for extended time periods on docks, at rail yards, and at industrial storage facilities;

FIG. **16** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the integration of the detection system with a satellite and monitoring equipment at a monitoring site for detecting explosives placed in a vehicle and then transmitting signals to the satellite and then to the monitoring site for disabling and locking the vehicle;

FIG. **17** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of the features and elements of the detector case to a cell phone and cell phone case;

FIG. **18** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of a GPS satellite, a monitoring site and a cell phone tower for communicating to and with an

electronic device such as a laptop computer or a cell phone for transmitting signals to a vehicle for activating an onboard stall-to-stop device for bringing the vehicle to a halt; and

FIG. **19** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the use of a GPS satellite in conjunction with the monitoring site and monitoring equipment to relay commands and signals to the cpu or transceiver of the vehicle for stopping or locking the vehicle in response to a signal that a certain type of event (detection of a bomb, engine failure or malfunction or unauthorized use) has occurred or is in process.

DETAILED DESCRIPTION OF REPRESENTATIVE EMBODIMENTS

Illustrated in FIGS. **1-19** is a multi-sensor detection and lock disabling system **10** for preventing terrorist activity by monitoring, detecting, and securing those critical areas; sites, and facilities vulnerable to terrorist activity. The first step is the identification of critical areas, sites, locations and facilities that are vulnerable to terrorist activity as convenient places to store and plant explosives and bombs and spread biological, chemical or radiological agents and compounds, followed by the disposition of the multi sensor detection and lock disabling system **10** for monitoring, detecting, and securing the particular location or site. Vulnerable sites, locations, facilities and areas are nearly limitless in their variety; in order to categorize the protection the present invention provides an anti-terrorist product grouping strategy has been developed wherein products made from the same or similar material, products having the same or similar design, and products presenting the same or similar security problems are grouped together with the multi sensor detection and lock disabling system **10** for preventing terrorist activity. For example, two preferred product groupings can be Product Grouping I: cargo containers, shipping containers, cargo planes, freight train cars, tractor trailers, mail carriers (UPS, FedEx), airport lockers, news racks (coin and non-coin operated), mail drop boxes, cluster mail boxes, keyed mail boxes, min-storage houses and buildings, bicycle lockers, stadium lockers, school lockers, cars, trucks, campers, buses, vans and utility vehicles. Product Grouping II: chemical detectors, biological detectors, radiological detectors, nuclear detectors, motion sensors, glass break sensors, plastic film on glass, high security locks, tampering labels, door sensors, disabling locking systems, vehicle detectors and satellite disabling locking systems. In addition to grouping products together by features, designs and materials, the multi sensor detection system **10** includes a lock disabling capability for disabling an existing lock or activating a lock on or inside any of the aforementioned products when a detector or sensor of the system is activated. The lock disabling feature is a crucial component of the invention in so far as it prevents unauthorized, unequipped or untrained individuals from gaining access and entry to the site and causing further contamination of the site.

As shown in FIGS. **1-10**, the multi sensor detection and lock disabling system **10** includes at least one—and preferably many—detector case **12** that can be placed in, on, upon or adjacent the product, such as the shipping containers **14** of FIGS. **4** and **5** resting upon a platform **16** or the cargo container **18** of FIG. **6** sitting upon a seaport dock or pier **20**. The detector case **12** includes a top **22**, a bottom **24**, a pair of opposed sides **26** and a front side or panel **28** and an opposite rear or back side **30**. The rear side **30** has connections or contacts that can include an Internet connection **32**, a GPS connection **34** and a power connection **36** for a power source. The power source for the detector system **10** can be any conventional battery or electrical source. The detector case **12** includes an interior chamber divided into a number of compartments **38** for holding therein agent or compound detection means hereinafter further described. A cpu **40** is mounted within the detector case **12** and electrically interconnects, routes, and transmits signals among items hereinafter further described and also communicates with a monitoring site and monitoring equipment. The front side **28** of the detector case **12** includes indicator means for visually indicating that a specific agent, compound or element has been detected. The indicator means can include color coded indicator lights **42** in panel form, as shown in FIG. **9**, with each indicator light panel **42** lighting up with a specific color corresponding to the detection of a specific agent or compound; or color coded indicator lights **44**, as shown FIG. **1**, that correspond to and individually light up on the detection of a specific agent or compound (chemical, biological, or radiological).

As shown in FIGS. **1**, **2** and **9-13**, the multi sensor detection and lock disabling system **10** includes a plurality of detectors **46** with each detector **46** adapted for and set up to sample for a specific agent or compound (biological, chemical, or radiological); and the detectors **46** are interchangeable for adapting to the needs and demands of future technology. The detectors **46** can also be used as stand-alone scanners. In the preferred embodiment of the invention, at least three detectors **46** are placed within the detector case **12** with one detector **46** for specifically sampling biological agents or compounds, one detector **46** for sampling chemical agents or compounds, and one detector **46** for sampling radiological agents or compounds. The detectors **46** are interconnected to the cpu **40** of the detection system **10** by conventional connections that can be wire or wireless for transmitting the appropriate signals to the cpu **40** upon detection of the particular agent or compound. As shown in FIG. **2**, each detector **46** includes on its front plate or facing surface a sound alarm indicator **48**, a readings panel **50** comprising a plastic shield and LED lights for displaying the various read-out messages, a sensor **52** for detecting the specific agent, element or compound, and a light alarm indicator **54** that can be color coded for each specific agent and which is externally visible when the detector **46** is used as a stand-alone scanner. Each detector **46** includes a conventional microprocessor for controlling the various functions and generating the appropriate signals for transmission to the cpu **40** of the detector case **12**.

As shown in FIGS. **1**, **3***a*, **3***b*, **9**, and **13-15**, used in conjunction with the multi sensor detection and lock disabling system **10** is at least one automatic/mechanical lock disabler **56**—and depending upon the number of products being monitored there can be one lock disabler **56** for each product. The automatic/mechanical lock disabler **56** is physically connected to the detector case **12** by a wire or cable **58** for receiving signals therefrom for disabling an existing lock or activating a lock inside a product to prevent access to the product. By way of example, FIG. **3***a* shows the automatic/mechanical lock disabler **56** mounted—by any conventional means—to the lock **60** of the shipping container **14** shown in FIGS. **4** and **5** and connected by wire **58** to the cpu **40** of the detector case **12**. The lock disabler **56** is in the non-activated or disengaged state in FIG. **3***a*. FIG. **3***b* shows the automatic/mechanical lock disabler **56** mounted to the lock **60** of the shipping container **14** and in the activated or engaged state after detection of an agent or

compound by the system **10** thereby for locking or disabling the lock **60** of the shipping container **14** and preventing unauthorized entry and access by unauthorized, untrained and unequipped individuals. In FIGS. **3***a* and **3***b* the lock **60** secures doors of the shipping container **14** that can be slidably or pivotably opened and closed.

In addition to the automatic/mechanical lock disabler **56**, the multi sensor detection and lock disabling system **10** can also utilize a fingerprint biometric lock with disabler **62** as shown in FIGS. **1** and **14**. The fingerprint biometric lock with disabler **62** is interconnected to the cpu **40** of the detector case **12** for receiving transmissions therefrom after detection of an agent or compound has occurred so that the lock on the product can be locked or disabled. Moreover, resetting of the fingerprint biometric lock with disabler **62** occurs when the fingerprint of the individual is placed on the fingerprint-matching pad **64**, and if a match occurs with a known fingerprint stored by the cpu **40**, then the individual can reset the fingerprint biometric lock with disabler **56** by turning the manual lock disabler **66**. The fingerprint biometric lock with disabler **62** is mounted to the lock of the product in a manner similar to the mounting of the automatic/mechanical lock disabler **56** that is shown in FIGS. **3** and **3***b*.

FIGS. **4** and **5** show one manner of disposition or placement of the detector case **12** in relation to the product, i.e., the shipping container **14**, with the color coded indicator lights **42** externally viewable; FIG. **5** shows a number of shipping containers **14** each equipped with a detector case **12** and integrated with elements hereinafter further described for continuously monitoring the shipping containers **14** as they sit for an extended period of time on the truck or rail platform **16**. FIG. **6** illustrates several cargo containers **18** sitting on the shipping dock or pier **20**, with each cargo container **18** having a detector case **12** mounted thereon and integrated with and monitored by elements shown in FIG. **5** and hereinafter further described.

FIG. **7** illustrates a typical product from product grouping **1** that is monitored by the multi sensor detection and lock disabling system **10** of the present invention; specifically, FIG. **7** shows a news rack **68** with one automatic/mechanical lock disabler **56** mounted to and interconnected with the locking mechanism of the news rack **68**. As long as there is no detection of any agent or compound, the lock disabler **56** is in the disengaged state, and the individual can deposit the coin amount in the chute and then freely open the glass panel **70** by the handle **72** for removing a paper. However, the lock disabler **56** would be activated upon detection of the harmful agent or compound and receipt of a signal from the cpu **40** for locking or disabling the locking mechanism thereby denying access to the interior of the news rack **68** from all untrained, unauthorized and unequipped individuals.

FIG. **8** illustrates one detector **46** disposed within the news rack **68** and which is visible through the panel **70** for detecting one specific agent, compound or element. The detector **46** functions as a stand-alone scanner and can be wirelessly interconnected to offsite monitoring equipment.

FIG. **11** illustrates a representative schematic **74** for describing the signal transmission process from the detector **46** to the cpu **40** of the detector case **12**. The external stimulus **76** would be the chemical, biological or radiological agent or compound. If there is no detection of the agent or compound, the detector **46** will stay in the sensing mode **78**. However, detection of the specific agent will trigger the sound alarm **80** and the light alarm **82**, and instant transmittal of a signal to the cpu **40**. The readings **84** can be stored by the cpu **40** for verification and future review and evaluation. After all the appropriate corrective and preventative measures have been undertaken by the trained and authorized personal, and the site has been cleansed of the contamination, authorized and equipped personal can then reset **86** the system **10**.

FIG. **12** illustrates a representative schematic **88** for the detector **46** when used as stand-alone scanner. The detector **46** undergoes the same essential steps as illustrated in FIG. **11**, with the exception of the signal transmission to the cpu **40**. The detector **46** remains in detection mode **78** until an agent is detected, and then the various functions-light alarm **82**, sound alarm **80**, storage of readings **84**, and, after the appropriate security and safety steps have been carried out by authorized personal, detector reset **90** by authorized personal can occur thereby placing the detector **46** back in detection or sensing mode **78**.

FIG. **13** is a representative schematic **92** that illustrates the steps undertaken by the system **10** to lock or disable a lock, such as the lock **60** for the shipping container **14** shown in FIGS. **3***a* and **3***b*. Upon detection of the agent (chemical, biological, radiological) the alarm light indicators **42** or **44** will light up providing external indication that an agent has been detected. In addition, the system **10**—the cpu **40**—will transmit a lock/disable lock signal **94** to the automatic/mechanical lock disabler **56** to lock or disable the lock on the product, such as the lock **60** on the shipping container **14** of FIGS. **3***a*-**5**. This prevents unauthorized, unequipped, or untrained individuals from entering or gaining access to the product for which a dangerous and perhaps lethal agent has been detected. After the proper authorities and authorized personal have been notified and all the appropriate security, preventative and clean up measures have been undertaken, the authorized individual can perform the disarm and reset function **96** for the system **10** placing the system **10** in back in the detection mode **98**.

FIG. **14** is a representative schematic **100** illustrating the use of the fingerprint biometric lock with disabler **62** with the system **10**. Upon detection of the agent or compound by the detector, the various alarms would sound and light up (shown in previous figures), and the cpu **40** would then transmit a signal to the fingerprint biometric lock with disabler **62** to lock or disable the lock on the product, such as the lock **60** on the shipping containers **14** shown in FIGS. **3***a*-**5**. The shipping containers **60** would remain locked and in an access denied mode **101** should an attempt be made to gain access to the container **60** by opening the lock **60** with an unauthorized fingerprint. However, a fingerprint that matches stored and authorized fingerprints **102** would indicate an authorized individual, and would allow the individual to disable and disarm **104** the lock **60** of the shipping container **14**. The fingerprint biometric lock with disabler **62** would then be reset **106** after the appropriate safety, cleanup, and protection measures are completed, and the system **10** would be reset and placed back in the detection mode **108**.

FIG. **15** is a schematic representation **110** that illustrates the integration of a surveillance watchtower **112** and a monitoring terminal or PC **114** for monitoring products such as the shipping containers **14** or cargo containers **16** that sit for extended periods of time of docks, piers **20**, truck terminals, rail yards, shipping platforms **16** and industrial sites as shown in FIGS. **5** and **6**. The watchtower **112** would maintain continuous surveillance over a number of shipping containers **60**, for example, with detector cases **12** mounted in or on each container **14** and set in detection mode **116** with one or more detectors **46** disposed in each detector case **12**. The watchtower **112** would continuously scan for light alarm indicators **42** and **44** on the products, such as the containers

14 or 18, and the watchtower 112 would be interconnected and integrated with the monitoring terminal or PC 114. Upon detection 118 of an agent or compound in one or more of the shipping containers 14, the appropriate light alarm indicators 42 or 44 would light providing visible confirmation of the detection of the specific agent or compound. The cpu 40 would transmit a lock/disable signal 120 to the lock 60 on each respective shipping container 14 to lock or disable the lock 60 thus preventing access to that respective shipping container 14. In addition, signal transmissions would be sent to the monitoring terminal or PC 114 (which could be off site) thereby alerting authorized security personal of the contamination event. With the information received at the monitoring terminal 114, authorized personal would then be notified and dispatched to the area to undertake the appropriate safety and cleanup measures 122. Such measures would also include disarming the lock disabling system in order to gain access to the shipping container 14. After all the cleanup and security measures are completed by the trained and properly equipped authorities, the detection system and the lock disabling feature would reset 124 and the detection system would again be placed in detection mode 116.

FIG. 16 is a schematic representation 126 that illustrates an enhanced version of the multi sensor detection and lock disabling system 10 for preventing car and vehicle attacks and bombings. The lock disabling system 10 would be interconnected to the locking system and mechanism 128 of the vehicle 130. In addition, a stall to stop disabling link 132 can be made with the fuel, air, and electrical system 134 of the vehicle 130. The enhanced version incorporates a satellite 136 for signal receipt and transmission from the vehicle 130 in which the detector system 10 is placed to a monitoring site and monitoring equipment 138. As shown in FIG. 16, a detection signal 140 would be sent to the satellite 136 by the detection system 10 upon detection of a bomb or explosive 142 hidden in the vehicle 130. The satellite 136 would then transmit an alert signal 144 to the monitoring site 138 with the signal 144 containing the relevant data to evaluate the nature of the threat. The monitoring site 138 would then transmit a stall to stop signal 146 to the detection system 10 to lock the vehicle 130 and/or disable the electrical system of the vehicle 130 thereby disabling the vehicle 130, preventing access to the vehicle 130 by locking the vehicle 130, and preventing any terrorist in the vehicle 130 from escaping.

The detector case 12 can be modified and adapted for inclusion with cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, suitcases; and briefcases. In addition, the basic monitoring terminal or PC 114, as shown in FIGS. 5 and 15, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring.

The system 10 and the watchtower 112, along with the satellite 136 and the monitoring site 138 can be adapted or incorporated with cell phone towers and satellites for use with satellite communication and/or a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency interconnected to a central processing unit (cpu), such as cpu 40, or a transceiver and monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween. The aforementioned telecommunication and radio communication means can be interactive with any type of motive vehicle that includes but is not limited to cars, trucks, vans, SUVs, trains, subways, boats, ships and airplanes, and which is reported stolen, experiences a loss of brakes, or a bomb, explosives or other types of chemical, biological, radiological, or nuclear agents are detected within, upon, affixed or mounted to the vehicle and which detection causes an automatic signal transmission or a signal transmission is activated when a call is made to the monitoring station by an authorized person. The authorized individual includes but is not limited to the owner, pilot, conductor, captain, police highway patrol, security guard and military personnel to the monitoring equipment for activating a vehicle slowdown or stall-to-stop disabling system that similar to the disabling system 126 shown in FIG. 16, or incorporating features of the system 126 shown in FIG. 16, from the monitoring equipment to the vehicle. The activation of the stall-to-stop disabling means or the vehicle slowdown disables or engages the computer, electrical, fuel and air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to the brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and the horsepower of the motor.

In addition, the basic stall-to-stop disabling means or the vehicle slowdown means and device can be adapted, modified or designed to include: an open bust or open platform for integrating any new and innovative technology; warning lights indicators; sound alarm indicators; voice alarm indicators; a cell phone to transmit to the vehicle a signal for slowing and halting the vehicle; and a lock disabling system or means to lock a thief or terrorist inside the vehicle after a transmission is received or sent. Open bust or open platform also refers to the compatibility of the detector case 12, or the incorporation of its features in cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, briefcases, and suitcases, etc., with other communication, transmission and surveillance systems whereupon the detector case 12, and its features, can be seamlessly integrated with other new and emerging systems and technologies.

Thus, as shown more specifically in FIG. 17, by way of a representative example the features and elements of the detector case 12 are shown as being incorporated into cell phone detector case 150 and associated cell phone monitor 152. The cell phone monitor 152 includes the standard keypad functions 154 and more specialized system use (ring tone, email, photos, texting) functions 156 as well as a viewing screen 158. The cell phone detector case 150 includes a recharging cradle or seat 160, a front side 162, a top 164, a bottom 166, and a pair of opposed sides 168. At the back of the cell phone detector case 150 are connections, contacts, and ports for at least an Internet connection 170, a GPS connection 172, and a contact, plug, or port for a power source 174. The power source for the cell phone detector case 150 can be any conventional rechargeable battery source or standard electrical power from a standard electrical receptacle or outlet.

As shown in FIG. 17, the cell phone detector case 150 includes one or more sensor/detector units, cells, or components 176 built into and incorporated into the case 150. The detector 176 includes generally disposed at the front 162 of the case 150 the following types of indicators: a sound alarm indicator 178, a readings panel 180, a sensor 182 for detecting one or more specific types of agents, elements, chemicals, compounds, etc., and a light alarm indicator 184. The sensor/detector 176 will be interconnected to the power source 174. In addition, mounted on and externally visible on the sides 168 or front 162 of the case 150 are a plurality of color coded indicator lights 186 with

each light **186** corresponding to a specific agent, element, chemical, compound, etc., and lighting up when that agent is detected by the sensor/detector **176**. The color coded indicator lights **186** will be electrically interconnected to the sensor/detectors **176** via any standard microprocessor. The cell phone detector case **150** and cell phone monitor **152** thus comprise a hand-held, easily portable and transportable detection means that is both effective and unobtrusive in its disposition and use.

FIGS. **18** and **19** illustrate representative examples of the integration of portable electronic communication or telecommunication devices such as a cell phone **187***a* and/or a laptop computer **187***b* with the monitoring equipment **138** located at a predesignated monitoring site **188**, and operating in conjunction with either a satellite and/or a cell phone tower **190** to transmit and receive signals and commands among each other and to a vehicle **192**, such as a truck, as part of a stall-to-stop disabling system for slowing and stopping the vehicle **192** and locking a thief, terrorist, or unauthorized individual in the vehicle **192** if needed. A wide range of events can trigger and initiate the stall-to-stop system and the locking or lock disabling system and mechanism, and the event doesn't have to be limited to the detection of a bomb or a chemical, biological, or radiological agent, element, or compound. The events can include, but is not limited to, detection of an engine problem to engine failure to the unauthorized use (stealing) of the vehicle **192**. The vehicle **192** includes an electromotive system **194** that comprises, among other components, an onboard computer(s), electrical, fuel and air systems, as well as brakes, ignition, steering, and transmission. Also integrated with and capable of communicating with the vehicle's **192** electromotive system **194** is a stall-to-stop system while a lock disabling mechanism **196** is able to engage and disengage or disable the vehicle's **192** locking mechanism **198** upon receipt of the appropriate commands via a lock disabling communication channel or link **200**. This link **200** can also accommodate the stall-to-stop system commands and signals, and thus is a multi-channel communication link. A CPU or a transceiver **202** is programmed to receive signals from the cell phone tower **190** and/or to a GPS satellite **204** and is interconnected with the stall-to-stop system and the lock disabling system **196** via link **200** for engaging the electromotive system **194** and actuating the lock disabling system **196** to stop the vehicle **192** and lock inside the vehicle **192** anyone such as a thief, terrorist or other unauthorized individual.

A representative example for stopping, disabling, and locking the vehicle **192** that utilizes the cell phone tower **190** wherein the activation and/or distress signal **206** originates from the cell phone **187***a* or the laptop **187***b* and such activation signal **206** travels to the cell phone tower **190** that is nearest the current location of the vehicle **192**. A signal **208** is then transmitted to the monitoring site **188** and specific monitoring equipment **138** that can also include but is not limited to cell phones, laptops, desktop PC's, notebook PCs and LCD monitors. The monitoring site **138** then communicates by signal **210** to the GPS satellite **204** that an original or activation signal has been received and then the GPS satellite **204** locates and communicates by multiplex signal **212** with the CPU or transceiver **202** on the vehicle **192** and exchanges information on the type of problem, situation, location, and vehicle speed. The monitoring equipment **138** then transmits a signal **214** to the cell phone tower **190** that communicates with the transceiver **202** and/or CPU of the vehicle **192** to initiate or execute any commands that will actuate the stall-to-stop disabling link **200** and lock disabling system **196** for bringing the vehicle **192** to a halt and actuating the vehicle's **192** locking mechanism **198** for locking the thief, terrorist, or other unauthorized person inside the vehicle **192** if needed.

FIG. **19** illustrates a representative example wherein the stall-to-stop system and the lock disabling system **196** are utilized in conjunction with the GPS satellite **204**. In FIG. **19** a signal has traveled to the satellites nearest the vehicle's **192** current location and then the signal **218** has traveled to the monitoring equipment **138** and monitoring site **188** which can include but is not limited to satellite cell phones, satellite monitors, cell phones, laptops, desktop PC's, notebook PC's, and LCD monitors. The GPS satellite **204** then locates and communicates with the CPU and/or transceiver **202** on the vehicle **192** via a multiplex (two-way) signal **220** in order to exchange information on such distress and danger event parameters as the specific problem situation, location, and vehicle speed. The monitoring equipment **138** then transmits a signal **222** back to the GPS satellite **204** that in turn communicates via another signal **224** with the CPU and/or transceiver **202** to execute any commands to the stall-to-stop system for executing the disengagement of the vehicle's **192** electromotive system **194** for bringing the vehicle **192** to a halt and for actuating the lock disabling system **196** to direct the lock disabling link **200** to actuate the locking mechanism **198** thereby locking the vehicle **192** and anyone inside the vehicle **192**.

The present invention comprehends a chemical/biological/radiological/nuclear/explosive/human/contraband detector unit with a disabling locking system for protecting products that can be grouped into several product groupings, from terrorist activity, and also for preventing unauthorized access to and tampering with the storage and transport of ordnance and weapons. The products grouped into what may be referred to as Product grouping 1 (storage & transportation) include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes, airplanes, subways, cargo planes, freight train cars, United Parcel Services™ (UPS™), Federal Express™ (FedEx™), airport lockers, news racks (coin and non-coin operated), mail drop boxes, cluster mail boxes, keyed mail boxes, min-storage houses and buildings, bicycle lockers, stadium lockers, school lockers, cars, trucks, campers, buses, vans, unmanned aerial vehicles (UAVs), unmanned ground vehicles (UGVs), and utility vehicles; the products grouped into what may be referred to as Product grouping 2 (sensors) include, but are not limited to, chemical, biological, radiological, explosive and nuclear detectors, motion sensors, door sensors, speed sensors, biometric sensors, glass break sensors, plastic film on glass, high security locks, tampering labels, door sensors, disabling locking systems, vehicle detectors and satellite disabling locking systems, detection of humans, detection of contraband, temperature, and shock levels; the products grouped into what may be referred to as Product grouping 3 (detector case; modified and adapted) include, but are not limited to, cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, suitcases, eyeglass, briefcases, detector cases of locks, detector cases of tags, detector cases that is mounted to, detector cases that is affixed to, detector cases that is outside of, detector cases that is inside of, and detector cases that is adjacent to; the products grouped into what may be referred to as Product grouping 4 (monitoring & communication devices) include, but are not limited to, mobile communication devices, mobile communication units, portable communication devices, portable communication equipment, wired communication devices, wireless

communication devices, monitoring sites, monitoring terminals, web servers, desktop personal computers (PCs), notebook personal computers (PCs), laptops, satellite cell phones, cell phones, Universal Mobile Telecommunications System (UMTS) phones, personal digital assistants (PDAs), liquid crystal display (LCD) monitors, and satellite monitoring, remote control key fobs, two-way communication key fobs, handhelds; the products grouped into what may be referred to as Product grouping 5 (communication methods) include, but are not limited to, Bluetooth, Wi-Fi, Wi-Max, Internet, Ethernet, Broadband, Network Bandwidth, Wireless, Wired, Text Messaging, Cellular, Satellite, Telematics, Wide Area Network (WAN), Wireless Wide Area Network (WWAN), Local Area Network (LAN), Radio Frequency (RF), Broadband Wireless Access (BWA), Global Positioning System (GPS), General Packet Radio Services (GPRS), Global System for Mobile (GSM), Wideband Code Division Multiple Access (W-CDMA), Universal Mobile Telecommunications System (UMTS), Short Message Service (SMS); the products grouped into what may be referred to as Product grouping 6 (biometrics) include, but are not limited to, fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature. the products grouped into what may be referred to as Product grouping 7 (authorized person) include, but are not limited to, owner, pilot, conductor, captain, drivers of vehicles identified as high security, airport security, police, highway patrol, security guard, military personnel, hazardous material (HAZMAT) personnel, the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), Secret Service, port security personnel, border security personnel, first responders, monitoring sites and terminal personnel. The multi sensor detection system includes the capability to disable an existing lock or activate a lock located inside or outside any of the products named in the product grouping categories upon activation of a sensor or detector included in the system. This is a significant feature for the multi sensor detection system as it prevents unauthorized, unequipped and untrained entry and access to the product thus preventing further contamination of the site and to individuals in the area.

While the invention has been shown and described in a preferred embodiment, it will be apparent to those skilled in the art that numerous alterations, modifications, and variations will possible and practicable without departing from the spirit and scope of the invention as set forth by the appended claims.

What is claimed:

1. A communication device that is at least a personal computer (PC), a cellphone, a smartphone, a laptop, or a handheld scanner, comprising at least a central processing unit (CPU), capable of:

processing instructions to lock, unlock, or disable the lock of the communication device;

processing instructions to activate a lock, unlock, or disabling lock means by engaging a vehicle with a two-way communication key-fob;

processing instructions to activate a start, stall, stop, or disabling means by engaging a vehicle's ignition system;

processing instructions to activate a lock, unlock, or disabling lock means; a start, stall, stop, or disabling vehicle means by engaging the operational systems of the unmanned aerial vehicle;

processing instructions to authenticate or identify a user by at least one of biometric fingerprint recognition, biometric facial recognition, biometric iris recognition, or biometric retina recognition;

processing instructions to scan a senor or tag using the short-range wireless technology of radio frequency near-field communication (NFC);

processing instructions to monitor or detect at least one of a chemical sensor, a biological sensor, a motion sensor, a biometric sensor, a signature sensor, or a human sensor;

processing instructions to monitor or detect for at least one of chemical agent, biological agent, radiological agent, nuclear agent, or explosive agent, weapons of mass destruction (WMDs);

processing instructions received through at least one of a Bluetooth, a Wi-Fi, a satellite, a global positioning system (GPS), or a cellular transmission;

processing instructions to connect the communication device to the internet or internet-of-things (IoTs) platform to sync, to at least one of a building's computer or security system, a vehicle's computer or security system, a lock, a detection device, or another communication device; and,

whereupon, the communication device is capable of processing instructions for operational and functional execution, and is capable of providing feedback of the execution, and storing the feedback into memory.

2. The communication device of claim 1, comprising at least a central processing unit (CPU), capable of processing operational instructions for at least a personal computer (PC), a cellphone, a smartphone, a laptop, or a handheld scanner.

3. The communication device of claim 1, comprising at least a central processing unit (CPU), capable of receiving a signal to lock, unlock, or disable the lock of the communication device.

4. The communication device of claim 1, comprising at least a central processing unit (CPU), capable of receiving a signal of at least fingerprint recognition, facial recognition, iris recognition, or retina recognition.

5. The communication device of claim 1, comprising at least a central processing unit (CPU), capable of receiving a signal of at least short-range wireless radio frequency near-field communication (NFC).

6. The communication device of claim 1, comprising at least a central processing unit (CPU), capable of receiving a signal from at least chemical sensor, biological sensor, motion sensor, biometric sensor, signature sensor, or human sensor.

7. The communication device of claim 1, comprising at least a central processing unit (CPU), capable of receiving a signal from at least one of chemical, biological, radiological, nuclear, or explosives detection.

8. The communication device of claim 1, comprising at least a central processing unit (CPU), capable of receiving a signal through at least a Bluetooth, a Wi-Fi, a satellite, a cellular, or GPS connection.

9. The communication device of claim 1, comprising at least a central processing unit (CPU), capable of receiving a signal of the communication device connection to the internet or internet-of-things (IoTs) platform to sync at least a building's computer or security system, a vehicle's computer or security system, a lock, a detection device, or another communication device.

10. The communication device of claim 1, comprising at least a central processing unit (CPU), capable of receiving a signal of the operational and functional execution of instruc-

tions; capable of providing feedback of the execution; and, capable of storing the feedback into memory.

11. A central processing unit (CPU) of at least a personal computer (PC), a cellphone, a smartphone, a laptop, or a handheld scanner, capable of:

processing instructions to lock, unlock, or disable the lock of the communication device;

processing instructions to activate a lock, unlock, or disabling lock means by engaging a vehicle with a two-way communication key-fob;

processing instructions to activate a start, stall, stop, or disabling means by engaging a vehicle's ignition system;

processing instructions to activate a lock, unlock, or disabling lock means; a start, stall, stop, or disabling vehicle means by engaging the operational systems of the unmanned aerial vehicle;

processing instructions to authenticate or identify a user by at least one of biometric fingerprint recognition, biometric facial recognition, biometric iris recognition, or biometric retina recognition;

processing instructions to scan a senor or tag using the short-range wireless technology of radio frequency near-field communication (NFC);

processing instructions to monitor or detect at least one of a chemical sensor, a biological sensor, a motion sensor, a biometric sensor, a signature sensor, or a human sensor;

processing instructions to monitor or detect for at least one of chemical agent, biological agent, radiological agent, nuclear agent, or explosive agent, weapons of mass destruction (WMDs);

processing instructions received through at least one of a Bluetooth, a Wi-Fi, a satellite, a global positioning system (GPS), or a cellular transmission;

processing instructions to connect the communication device to the internet or internet-of-things (IoTs) platform to sync, to at least one of a building's computer or security system, a vehicle's computer or security system, a lock, a detection device, or another communication device; and,

whereupon, the central processing unit (CPU) of the communication device is capable of processing instructions for operational and functional execution, and is capable of providing feedback of the execution, and storing the feedback into memory.

12. The central processing unit (CPU) of claim 11, capable of processing operational instructions for at least one of a personal computer (PC), a cellphone, a smartphone, a laptop, or a handheld scanner.

13. The central processing unit (CPU) of claim 11, capable of processing operational instructions to lock, unlock, or disable the lock of the communication device.

14. The central processing unit (CPU) of claim 11, capable of processing operational instructions of at least fingerprint recognition, facial recognition, iris recognition, or retina recognition.

15. The central processing unit (CPU) of claim 11, capable of processing operational instructions from short-range wireless radio frequency near-field communication (NFC).

16. The central processing unit (CPU) of claim 11, capable of processing operational instructions from at least chemical sensor, biological sensor, motion sensor, biometric sensor, signature sensor, or human sensor.

17. The central processing unit (CPU) of claim 11, capable of processing operational instructions from at least chemical, biological, radiological, nuclear, or explosives detection.

18. The central processing unit (CPU) of claim 11, capable of processing operational instructions through at least a Bluetooth, a Wi-Fi, a satellite, a cellular, or GPS connection.

19. The central processing unit (CPU) of claim 11, capable of processing operational instructions of the communication device connection to the internet or internet-of-things (IoTs) platform to sync at least a building's computer or security system, a vehicle's computer or security system, a lock, a detection device, or another communication device.

20. The central processing unit (CPU) of claim 11, capable of processing operational instructions of functional execution of instructions; capable of providing feedback of the execution; and, capable of storing the feedback into memory.

* * * * *

EXHIBIT M

Plaintiff's '891 Patent

US00RE43891E

(19) **United States**

(12) **Reissued Patent**
Golden

(10) **Patent Number: US RE43,891 E**

(45) **Date of Reissued Patent: Jan. 1, 2013**

(54) **MULTI SENSOR DETECTION, STALL TO STOP AND LOCK DISABLING SYSTEM**

(76) Inventor: **Larry Golden**, Mauldin, SC (US)

(21) Appl. No.: **13/065,837**

(22) Filed: **Mar. 31, 2011**

Related U.S. Patent Documents

Reissue of:

(64) Patent No.: **7,636,033**
Issued: **Dec. 22, 2009**
Appl. No.: **12/155,573**
Filed: **Jun. 6, 2008**

U.S. Applications:

(63) Continuation-in-part of application No. 11/397,118, filed on Apr. 5, 2006, now Pat. No. 7,385,497.

(51) **Int. Cl.**
B60R 25/10 (2006.01)
G08B 1/08 (2006.01)

(52) **U.S. Cl.** **340/426.11**; 340/426.16; 340/539.11

(58) **Field of Classification Search** 340/425.5, 340/426.11–426.19, 426.25, 521, 522, 539.1, 340/539.11, 539.13, 539.22, 539.26, 540, 340/545.3, 600; 701/29, 32, 36, 2, 29.1, 701/31.5, 32.2, 32.4, 32.9; 702/22; 307/10.2, 307/10.3

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,385,469	A	5/1983	Scheuerpflug
4,544,267	A	10/1985	Schiller
4,586,441	A	5/1986	Zekich
4,792,226	A	12/1988	Fishbine et al.
5,222,152	A	6/1993	Fishbine et al.
5,223,844	A	6/1993	Mansell et al.
5,233,404	A	8/1993	Lougheed et al.
5,557,254	A	9/1996	Johnson
5,682,133	A	10/1997	Johnson
5,766,956	A	6/1998	Groger et al.
5,938,706	A	8/1999	Feldman
5,963,657	A	10/1999	Bowker et al.
5,986,543	A	11/1999	Johnson
6,078,265	A	6/2000	Bonder et al.
6,271,745	B1	8/2001	Anzai et al.
6,374,652	B1	4/2002	Hwang
6,542,076	B1	4/2003	Joao
6,542,077	B2	4/2003	Joao
6,588,635	B2	7/2003	Vor Keller et al.

(Continued)

OTHER PUBLICATIONS

U.S. Appl. No. 12/802,001, filed May 27, 2010, Golden.

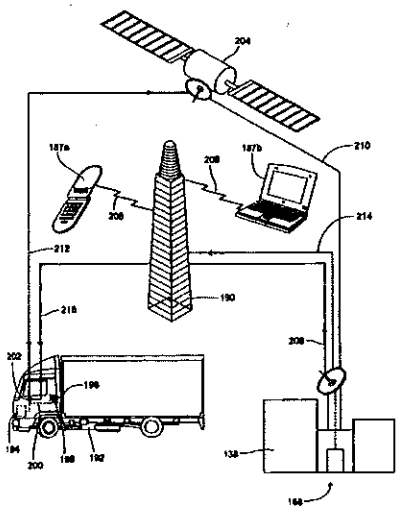
(Continued)

Primary Examiner — Van T. Trieu

(57) **ABSTRACT**

A multi sensor detection and disabling lock system includes detector cases for holding interchangeable detectors that sample for chemical, biological and radiological compounds, agents and elements, with each detector case disposed in or upon the monitored product whereupon light alarm indicators (color coded) on the detector case light up when a specific compound or agent is detected whereupon the detector case transmits detection information to a monitoring computer terminal and transmits a signal to a lock disabler engaged to the product to lock or disable the product's lock thereby preventing untrained, unauthorized and unequipped individual's from gaining access and entry to the product, and also preventing further contamination of the area. An authorized individual resets the detection system, and the system's power source is electrical, battery or computer generated. In addition, the detection system can be interconnected to surveillance towers scanning detector cases disposed at seaport docks, freight depots and rail terminals for monitoring containers being prepared for shipment or sitting on docks for long periods of time.

75 Claims, 13 Drawing Sheets



U.S. PATENT DOCUMENTS

6,610,977	B2	8/2003	Megerle	
6,613,571	B2	9/2003	Cordery et al.	
6,628,813	B2	9/2003	Scott et al.	
6,647,328	B2	11/2003	Walker	
6,738,697	B2 *	5/2004	Breed	701/31.5
6,923,509	B1	8/2005	Barnett	
6,980,092	B2	12/2005	Turnbull et al.	
7,005,982	B1	2/2006	Frank	
7,034,683	B2	4/2006	Ghazarian	
7,103,460	B1	9/2006	Breed	
7,109,859	B2	9/2006	Peeters	
7,116,798	B1	10/2006	Chawla	
7,346,439	B2	3/2008	Bodin	
7,385,497	B2	6/2008	Golden	
7,397,363	B2	7/2008	Joao	
7,636,033	B2	12/2009	Golden	
2003/0206102	A1	11/2003	Joao	
2004/0107028	A1	6/2004	Catalano	
2005/0195069	A1	9/2005	Dunand	
2006/0250235	A1	11/2006	Astrin	
2008/0122595	A1	5/2008	Yamamichi	
2008/0234907	A1	9/2008	Labuhn	
2010/0159983	A1	6/2010	Golden	
2011/0178655	A1	7/2011	Golden	

OTHER PUBLICATIONS

A newspaper article of Mr. Melvin Sullivan and his family that references the date, Mar. 6, 2001.

A letter of response Mr. Sullivan received from Pfeiffer & Gantt, PA, dated Sep. 16, 2002.

A "Certificate of Existence" Bright Idea Inventor, LLC. Nov. 6, 2002.

Operating Agreement of Bright Idea Inventor, LLC received from Pfeiffer & Gantt, PA, dated Nov. 13, 2002.

A "Membership Certificate" received from Bright Idea Inventor, LLC dated Nov. 13, 2002.

A letter of response Golden received from the Honorable Congressman from Maryland, Elijah E. Cummings, dated Dec. 16, 2002.

A newspaper article of Mr. Melvin Sullivan and Mr. Larry Golden, dated, Feb. 27-Mar. 5, 2003.

A letter of response Golden received from the Honorable Senator from South Carolina, Ernest F. Hollings, dated May 21, 2003.

A letter of response Golden received from the Office of the Vice President, Dick Cheney, dated Jun. 3, 2003.

A letter of response Golden received from the Honorable Senator from South Carolina, Ernest F. Hollings, dated Oct. 1, 2003.

A letter of response Golden received from the Honorable Senator from South Carolina, Lindsey O. Graham, dated Oct. 21, 2003.

A letter sent to the President of the United States George W. Bush, the President's Cabinet, the United States Senate and the Congressional Black Caucus, dated May 23, 2005.

On Nov. 17, 2004, "Disclosure Document Registration" was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.

On Jul. 10, 2005, an "Inventor's Official Record of Invention", was filed in my name (Golden) at "The Law Office of David P. Gaudio, P.C.; The Inventors Network."

On Aug. 23, 2005, "Disclosure Document Registration".

On Apr. 5, 2006, "Patent Application" was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.

On Jun. 06, 2008, "Continuance-In-Part, (CIP) Application" was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.

On Jun. 10, 2008, Golden was issued a Patent (7,385,497) the "Multi sensor detection and lock disabling system."

On Dec. 22, 2009, Golden was issued a Patent (7,636,033) the "Multi sensor detection, stall-to-stop, and lock disabling system."

On Jan. 20, 2010, a "Continuation Application" (U.S. Appl. No. 12/657,356) was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.

On May 27, 2010, a "Continuation Application" (U.S. Appl. No. 12/802,001) was filed in my name (Golden) at the United States Patent & Trademark Office in Washington, D.C.

Reissue of U.S. Patent No. 7,636,033; "Swear Back"; In accordance to Title 37—Code of Federal Regulations Patents, Trademarks, and Copyrights; Apr. 8, 2011.

Reissue of U.S. Patent No. 7,636,033; "Swearback—History of Work"; Apr. 8, 2011.

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 11/397,118; mailed Nov. 14, 2007; Alexandria, Virginia, USA; pp. 1-12; (12 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/155,573; mailed Apr. 9, 2009; Alexandria, Virginia, USA; pp. 1-7; (7 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/155,573; mailed Jul. 30, 2009; Alexandria, Virginia, USA; pp. 1-9; (9 pages).

United States Patent and Trademark Office; Notice of Allowability from U.S. Appl. No. 12/155,573; mailed Oct. 28, 2009; Alexandria, Virginia, USA; pp. 1-5; (5 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/657,356; mailed Jul. 12, 2010; Alexandria, Virginia, USA; pp. 1-14; (14 pages).

United States Patent and Trademark Office; Notice of Allowability from U.S. Appl. No. 12/657,356; mailed Mar. 10, 2011; Alexandria, Virginia, USA; pp. 1-4; (4 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001; mailed May 27, 2010; Alexandria, Virginia, USA; pp. 1-16; (16 pages).

United States Patent and Trademark Office; Office Action from U.S. Appl. No. 12/802,001; mailed May 27, 2011; Alexandria, Virginia, USA; pp. 1-14; (14 pages).

United States Patent and Trademark Office; Office Action; Office Action from U.S. Appl. No. 12/802,001; copyright and mailing date Dec. 12, 2011, pp. 1-9, publisher United States Patent and Trademark Office, Alexandria, Virginia, USA; (9 pages).

* cited by examiner

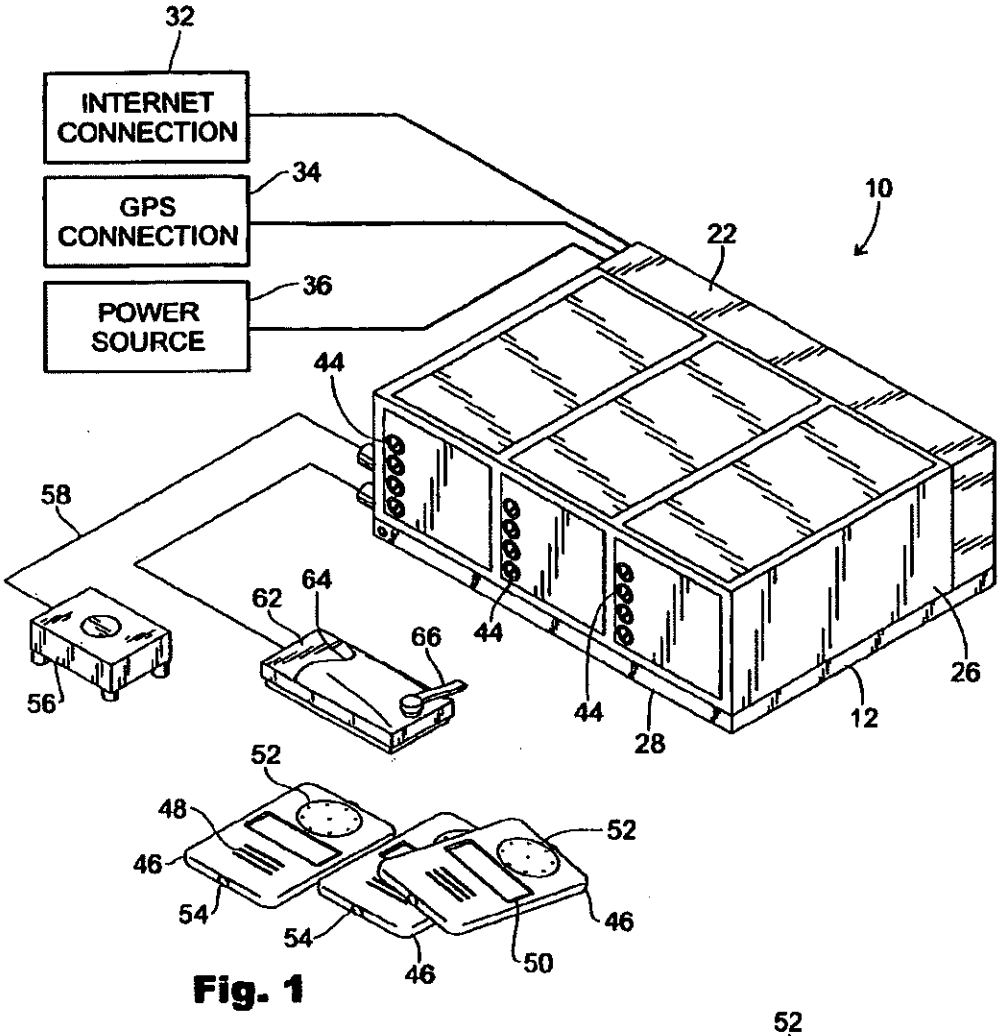

32
INTERNET CONNECTION
34
GPS CONNECTION
36
POWER SOURCE
10
22
44
58
62
64
66
56
44
28
12
26
52
48
46
54
54
46
50
52
46

Fig. 1

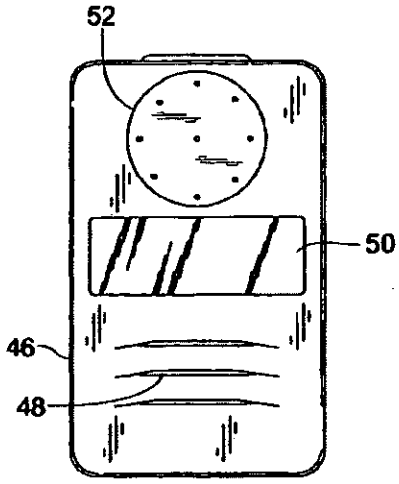

52
50
46
48

Fig. 2

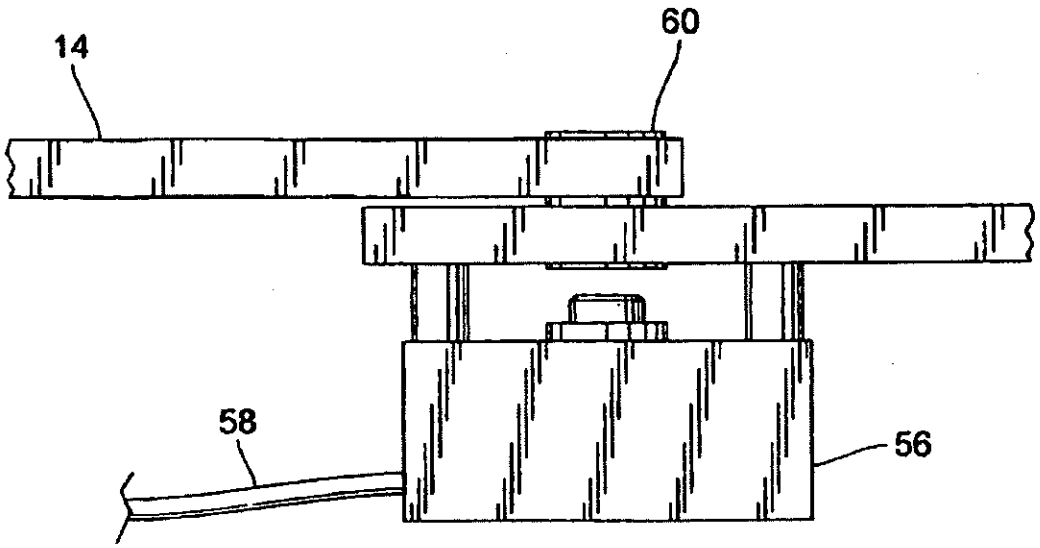


Fig. 3a

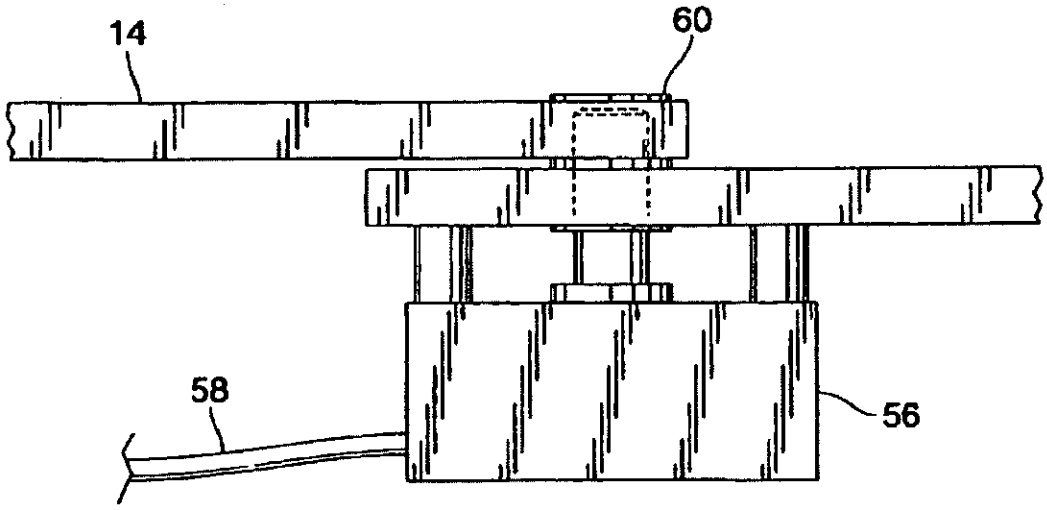


Fig. 3b

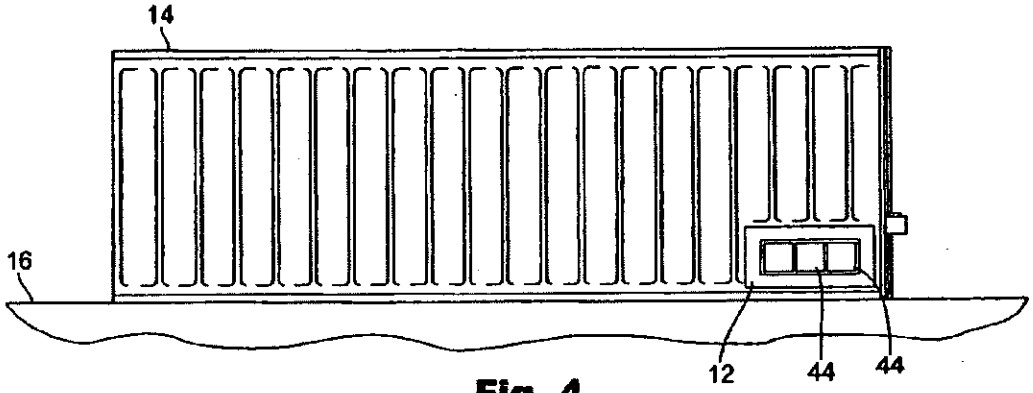


Fig. 4

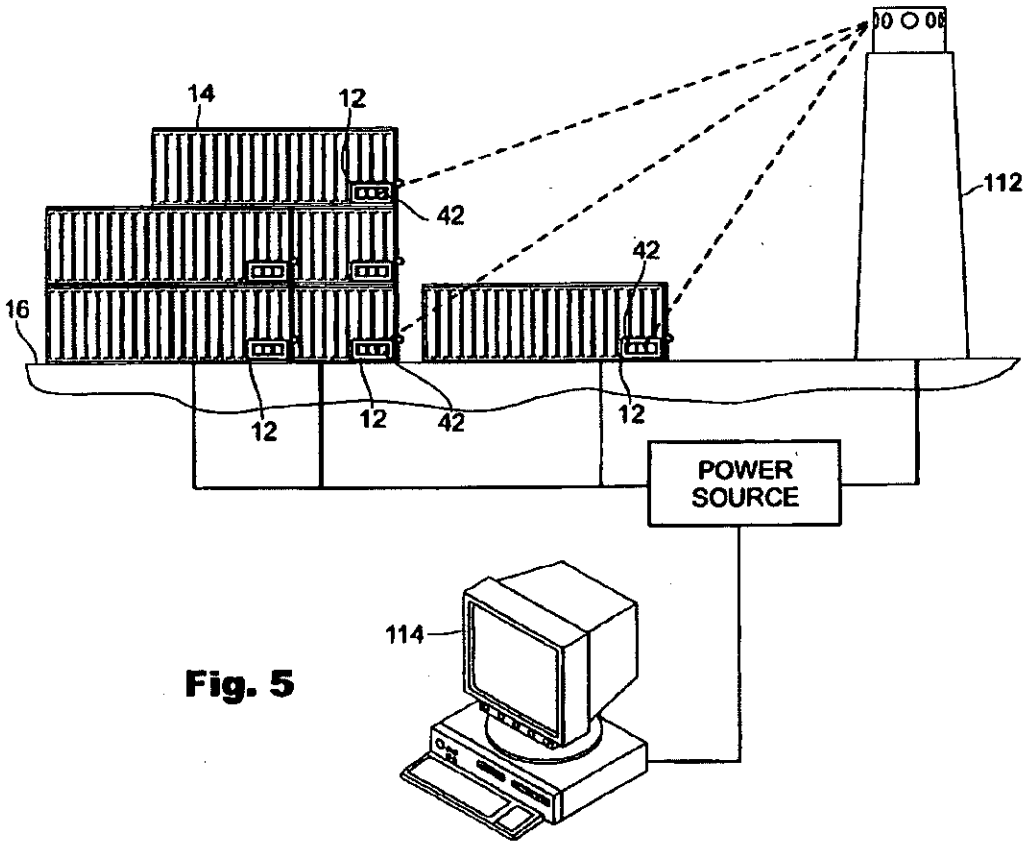


Fig. 5

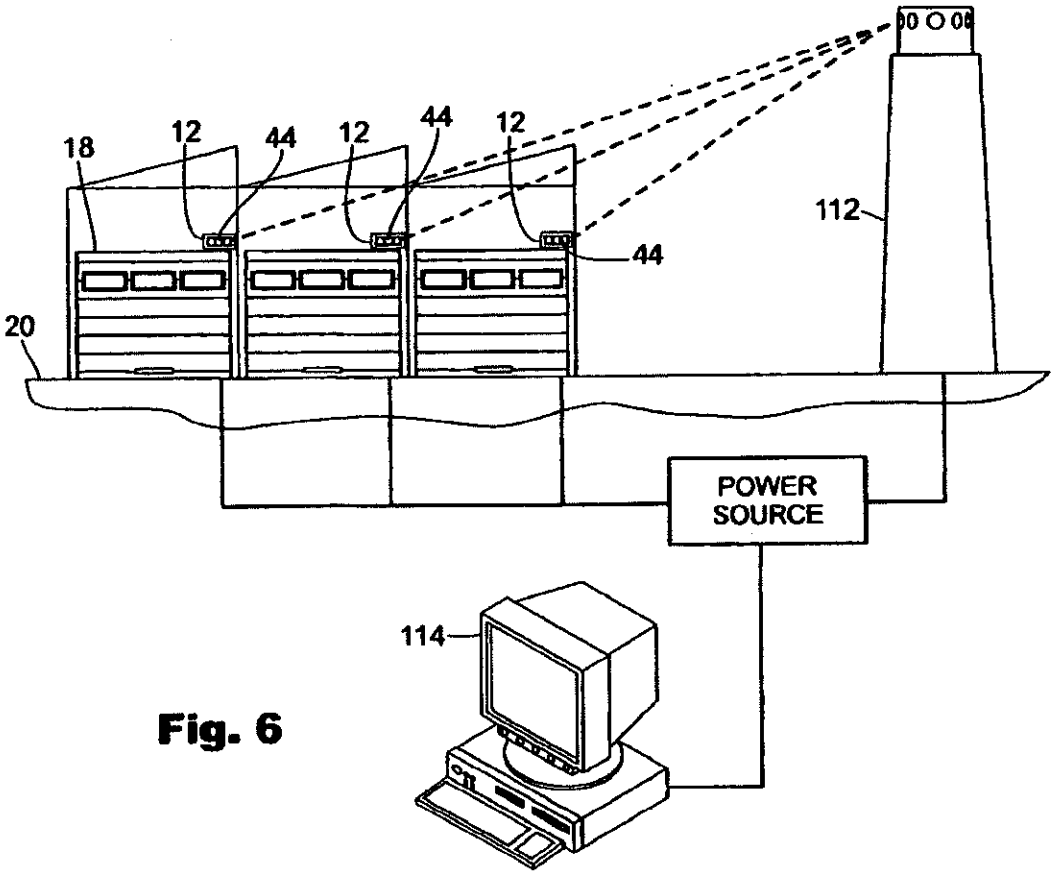


Fig. 6

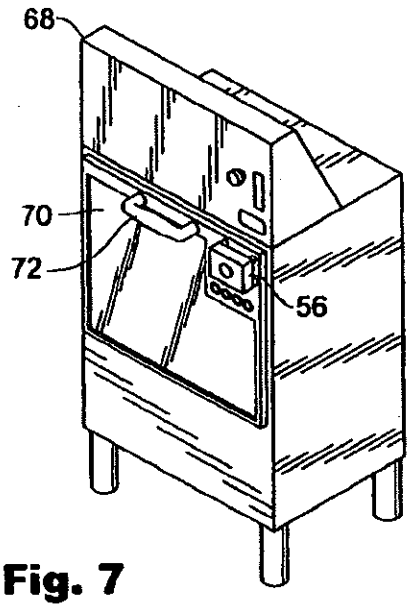


Fig. 7

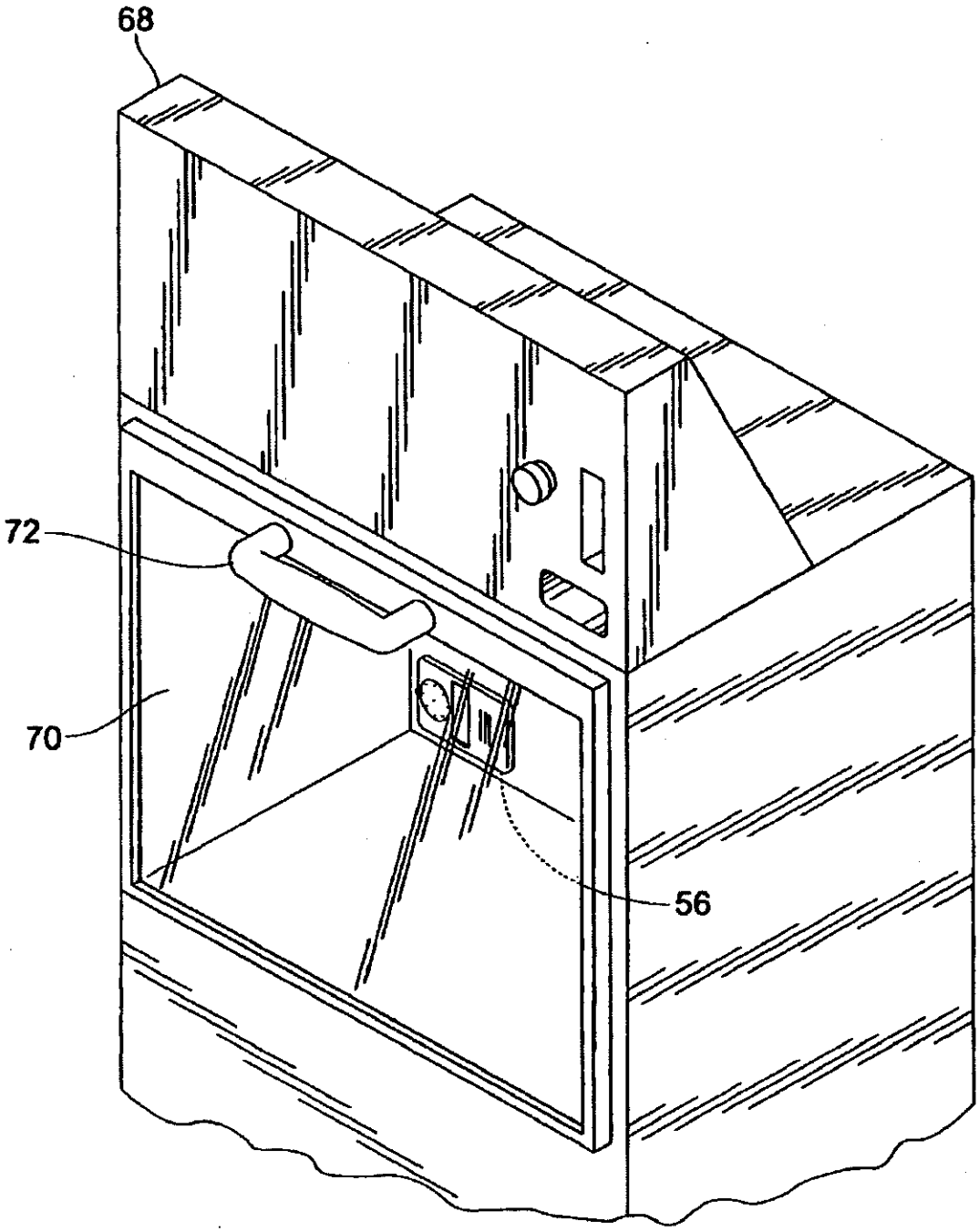


Fig. 8

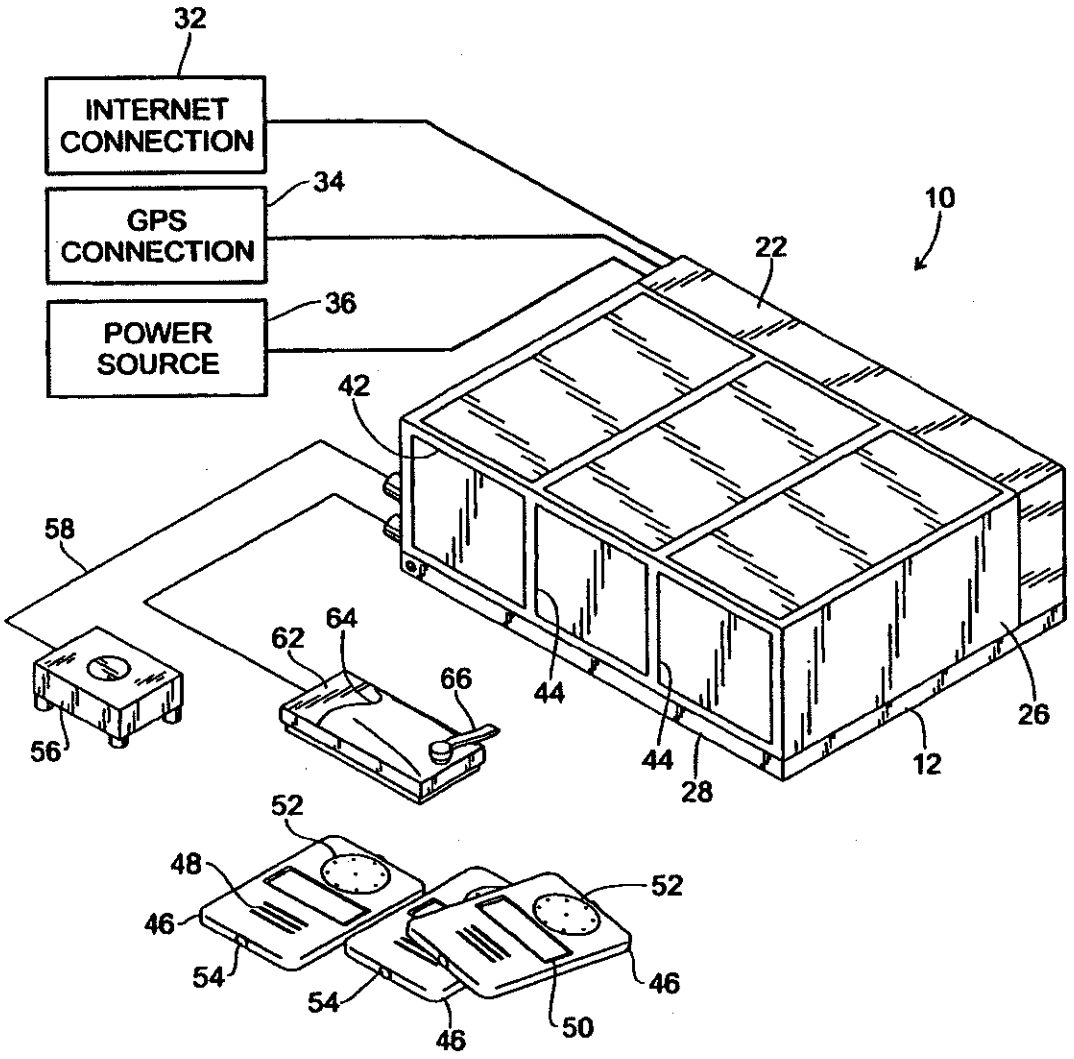

32
INTERNET CONNECTION
34
GPS CONNECTION
36
POWER SOURCE
10
22
42
58
62
64
66
44
56
26
44
28
12
52
48
46
54
52
46
54
46
50

Fig. 9

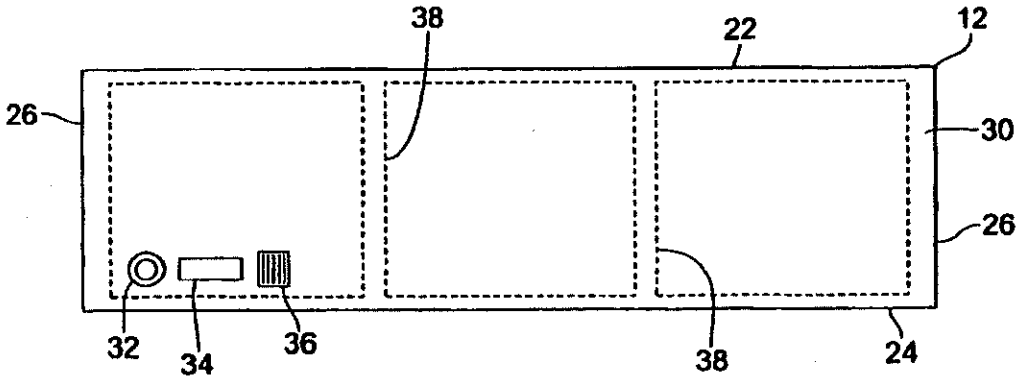

38
22
12
26
30
26
32
34
36
38
24

Fig. 10

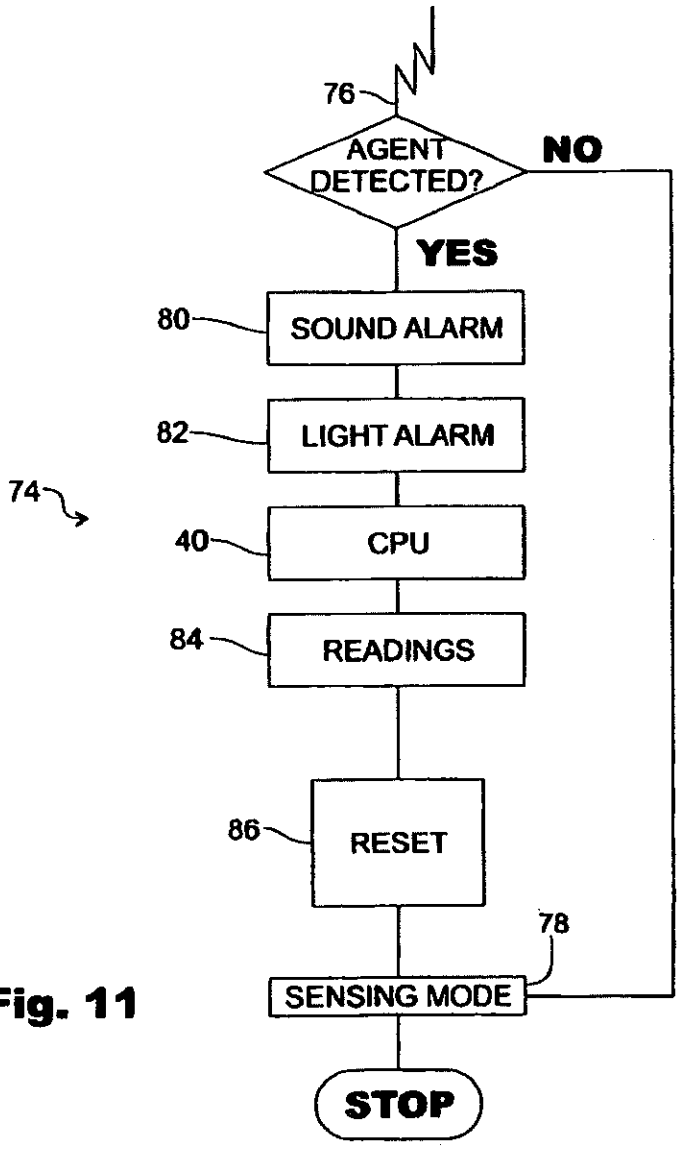

76
AGENT DETECTED?
NO
YES
80
SOUND ALARM
82
LIGHT ALARM
74
40
CPU
84
READINGS
86
RESET
78
SENSING MODE
STOP

Fig. 11

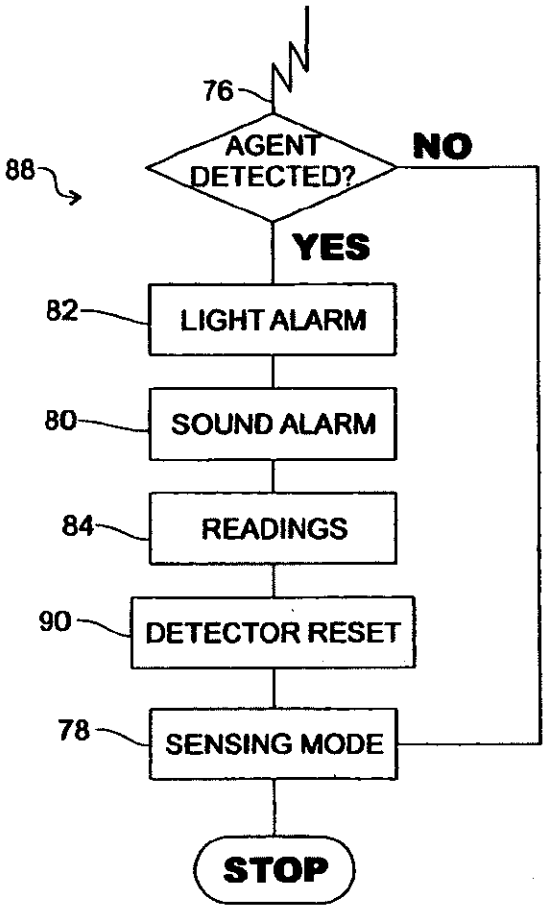

76
AGENT DETECTED?
NO
88
YES
82
LIGHT ALARM
80
SOUND ALARM
84
READINGS
90
DETECTOR RESET
78
SENSING MODE
STOP

Fig. 12

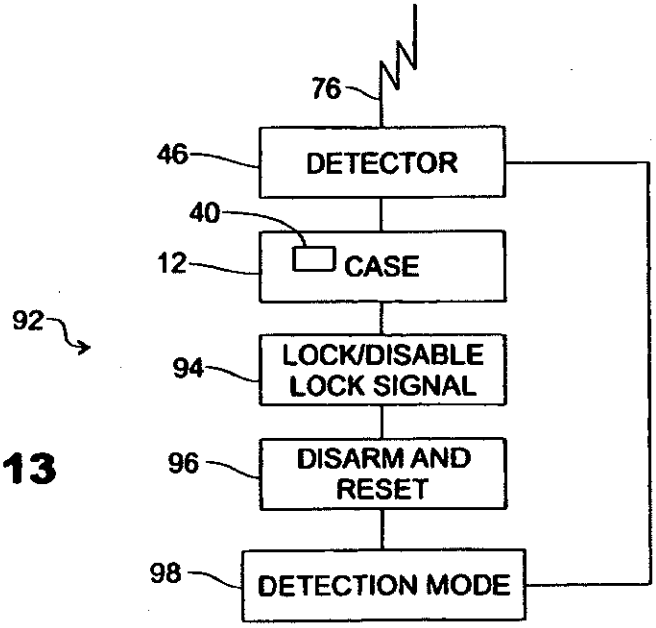

76
46
DETECTOR
40
12
CASE
92
94
LOCK/DISABLE LOCK SIGNAL
96
DISARM AND RESET
98
DETECTION MODE

Fig. 13

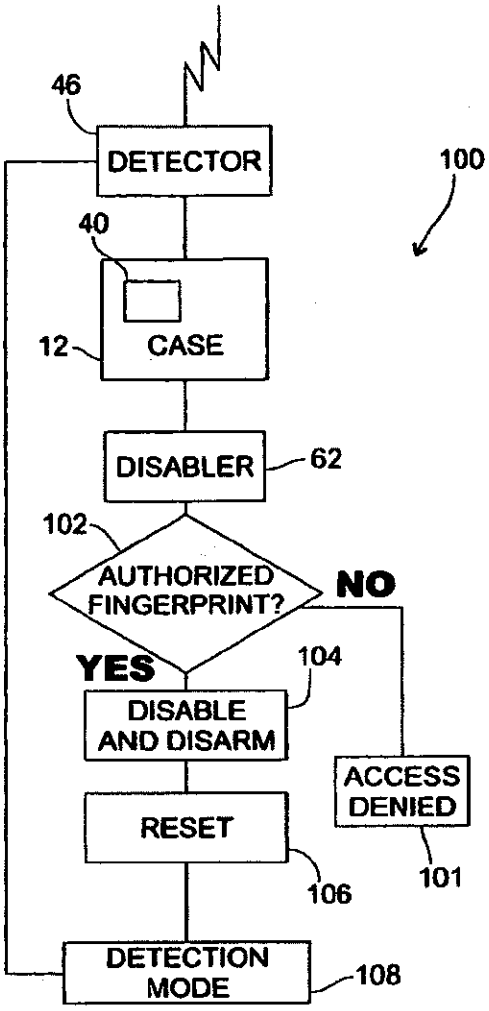

46
DETECTOR
100
40
CASE
12
DISABLER
62
102
AUTHORIZED FINGERPRINT?
NO
YES
104
DISABLE AND DISARM
ACCESS DENIED
101
RESET
106
DETECTION MODE
108

Fig. 14

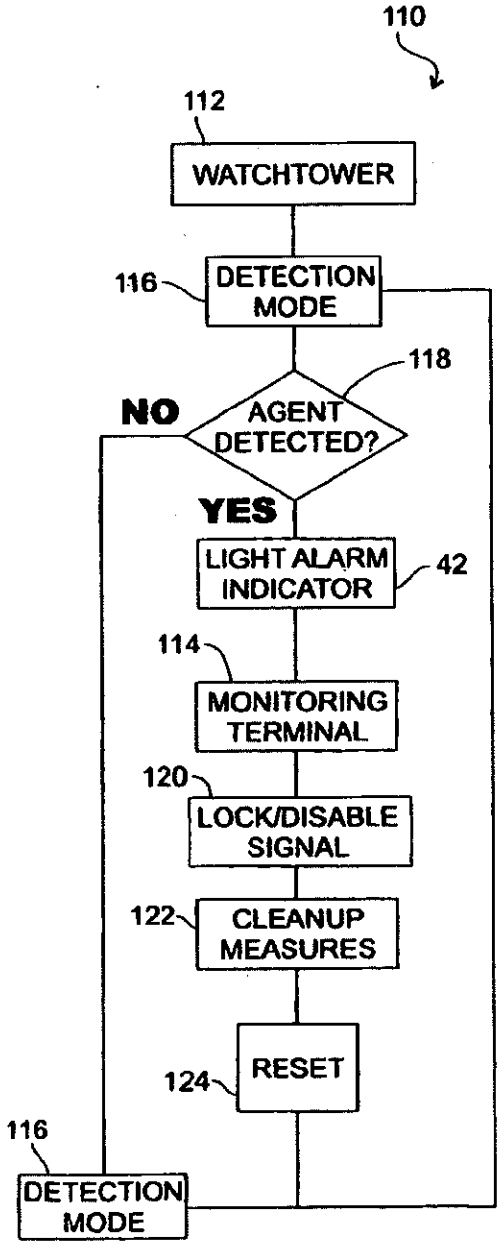

110
112
WATCHTOWER
116
DETECTION MODE
118
NO
AGENT DETECTED?
YES
LIGHT ALARM INDICATOR
42
114
MONITORING TERMINAL
120
LOCK/DISABLE SIGNAL
122
CLEANUP MEASURES
RESET
124
116
DETECTION MODE

Fig. 15

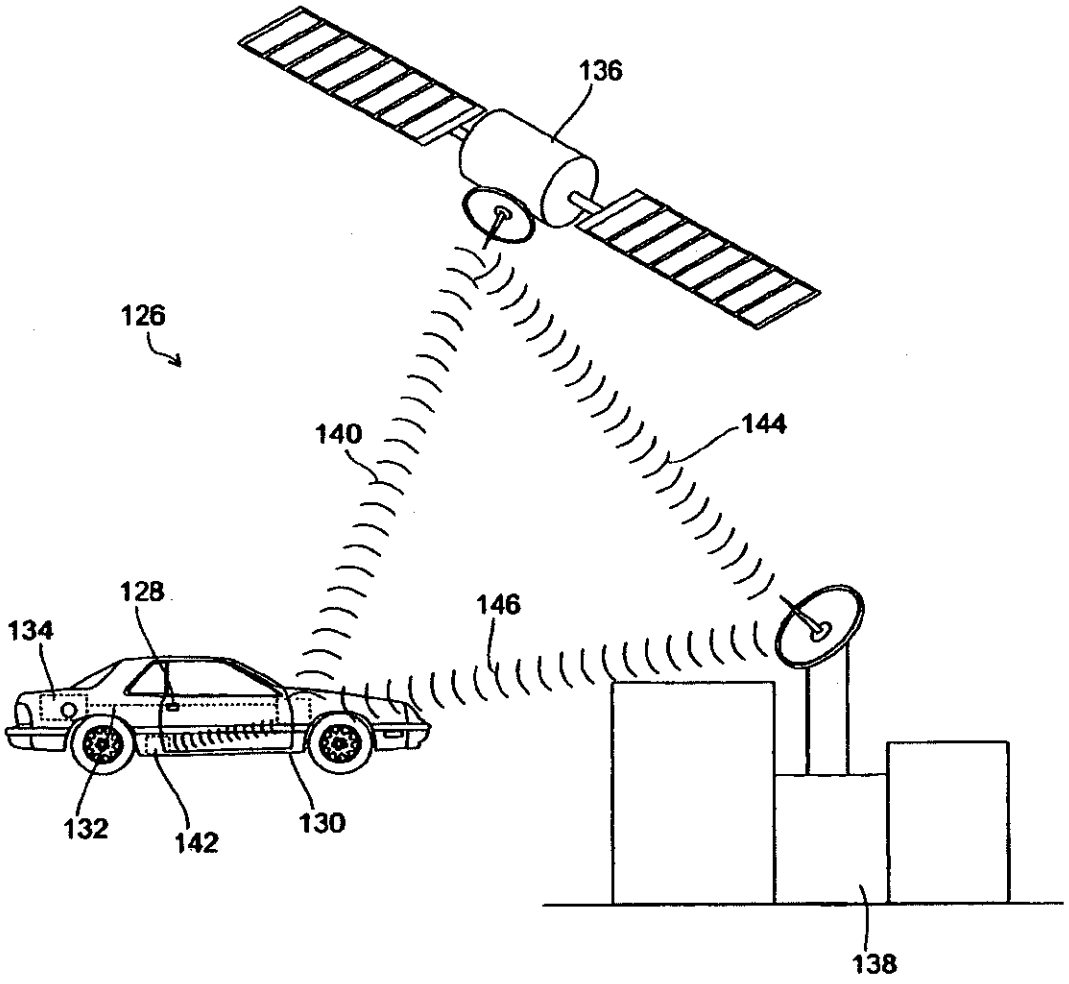


Fig. 16

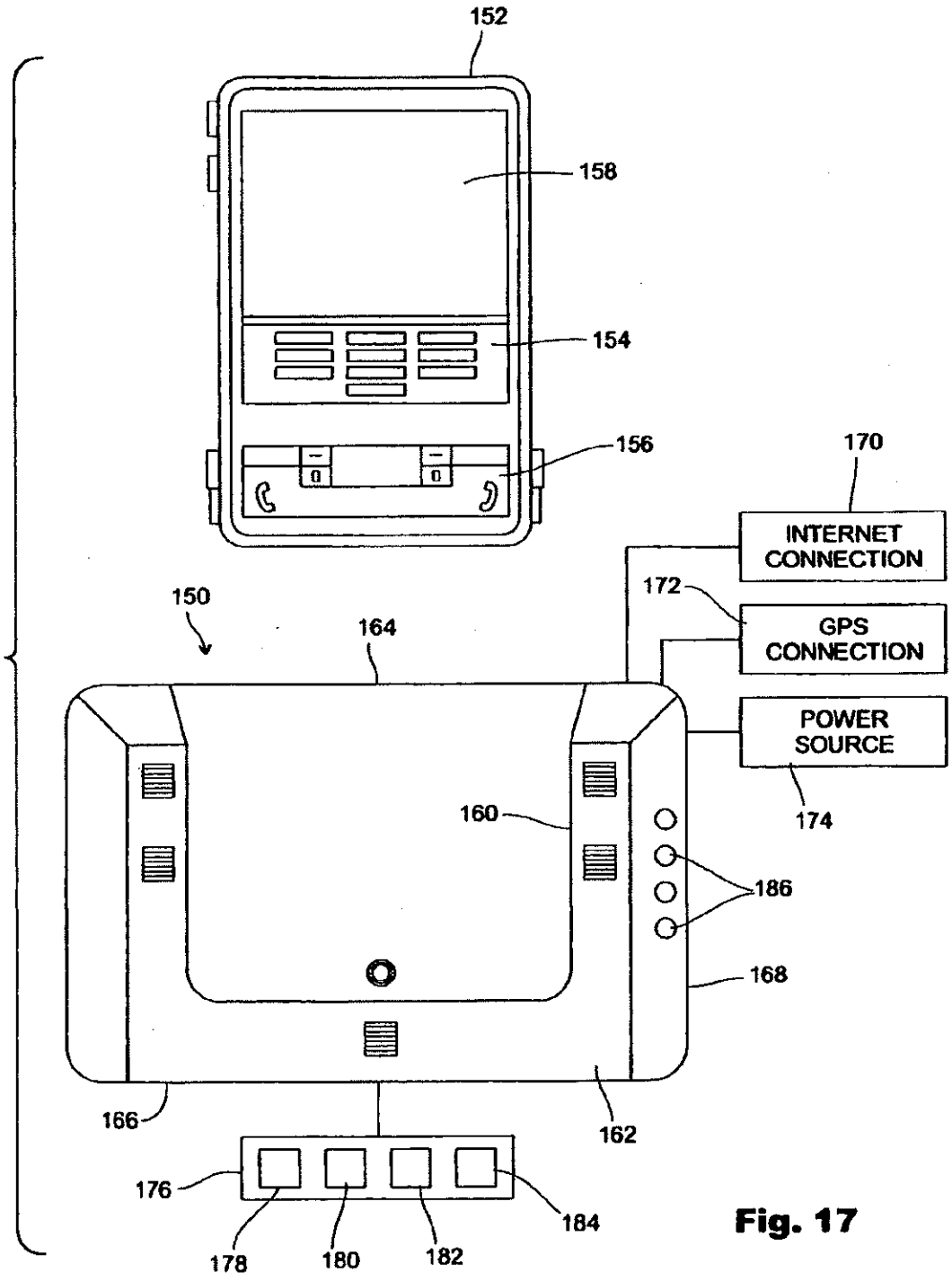

152
158
154
156
170
INTERNET CONNECTION
172
GPS CONNECTION
POWER SOURCE
174
150
164
160
186
168
166
162
176
184
178
180
182

Fig. 17

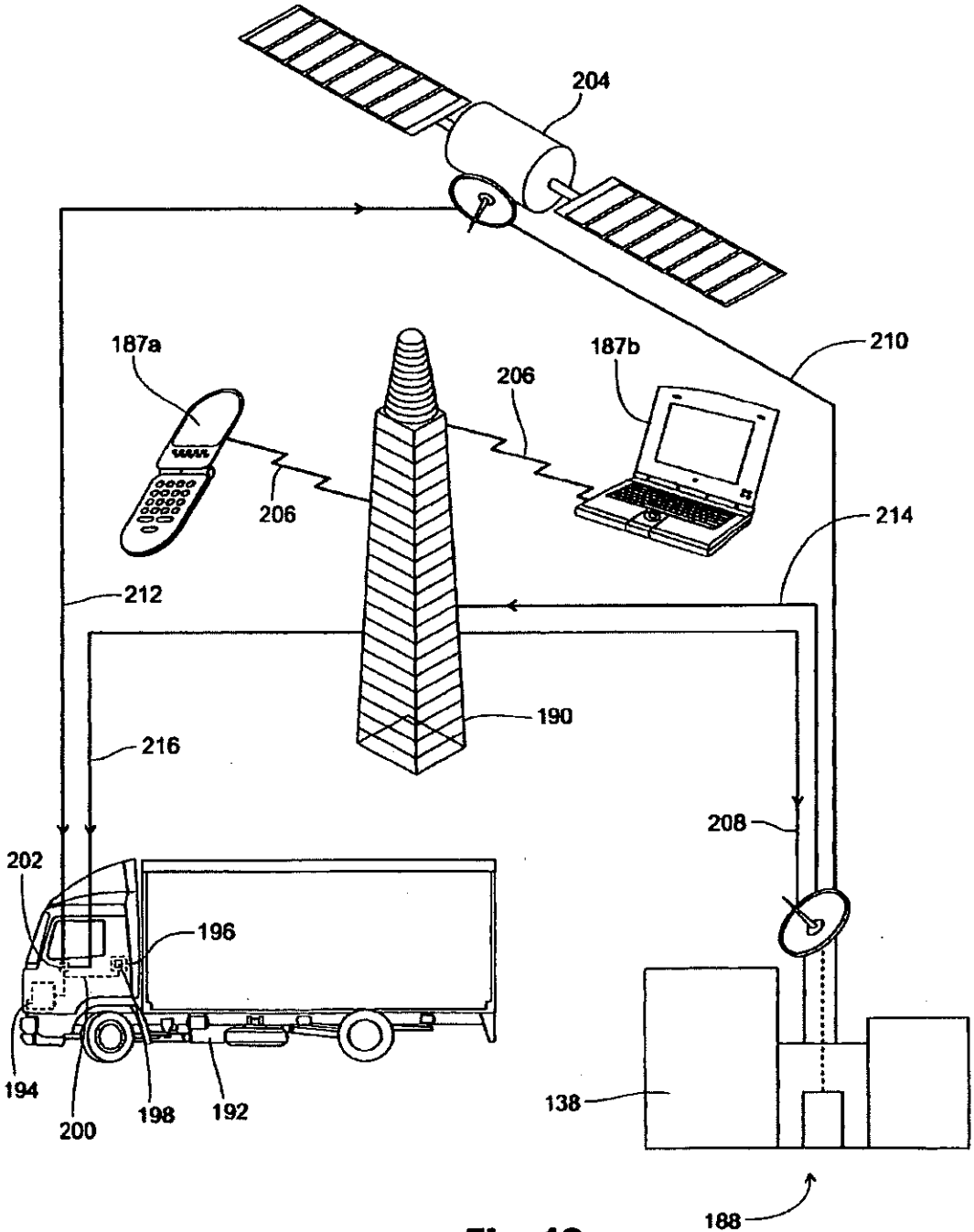

204
187a
187b
210
206
206
214
212
190
216
208
202
196
194
200
198
192
138
188

Fig. 18

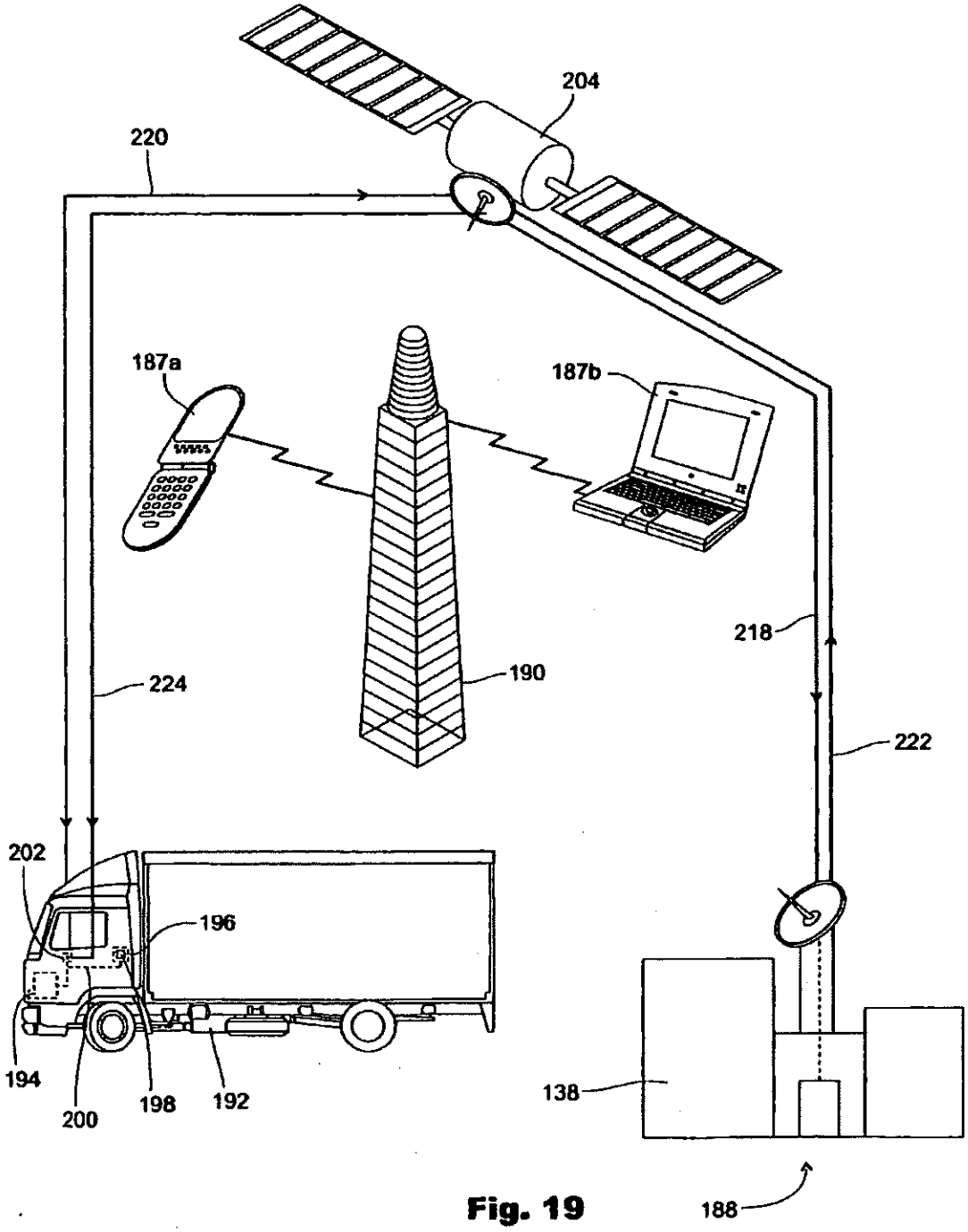

204
220
187a
187b
218
224
190
222
202
196
194
200
198
192
138
188

Fig. 19

MULTI SENSOR DETECTION, STALL TO STOP AND LOCK DISABLING SYSTEM

Matter enclosed in heavy brackets [ ] appears in the original patent but forms no part of this reissue specification; matter printed in italics indicates the additions made by reissue.

RELATED APPLICATIONS

[This application] *More than one reissue application has been filed for the reissue of U.S. Pat. No. 7,636,033 B2. The reissue applications are application Ser. No. 13/199,853 filed Sep. 9, 2011 which is a divisional reissue of U.S. Pat. No. 7,636,033 B2, and the present application Ser. No. 13/065,837 filed Mar. 31, 2011 which is a reissue of U.S. Pat. No. 7,636,033 B2. The present application is a reissue of U.S. Pat. No. 7,636,033 B2 and claims priority to this patent the entire contents of which are incorporated by reference in their entirety herein for all purposes. U.S. Pat. No. 7,636,033 B2* is a continuation-in-part of U.S. patent application Ser. No. 11/397,118 titled "Muti Sensor Detection and Lock Disabling System" filed on Apr. 5, 2006 and is now U.S. Pat. No. 7,385,497, the complete subject matter of which is incorporated by reference herein in its entirety. [This application] *U.S. Pat. No. 7,636,033 B2* is a continuation-in-part of U.S. patent application Ser. No. 11/397,118 and names as the inventor, Larry Golden, being the same inventor named in the aforedescribed prior application having the Ser. No. of 11/397,118, and thus [this application] *U.S. Pat. No. 7,636,033 B2* constitutes a continuation-in-part as set forth in 35 U.S.C. 120 and claims the effective filing date of prior application having Ser. No. 11/397,118 and is now U.S. Pat. No. 7,385,497.

FIELD OF THE INVENTION

The present invention pertains to anti-terrorist detection and prevention systems, and more particularly pertains to a disabling lock mechanism combined with a chemical/biological/radiological detection system for use with products grouped together by similar characteristics in order to prevent unauthorized entry, contamination and terrorist activity.

BACKGROUND OF THE INVENTION

Terrorist activity is a continuous, daily, worldwide threat to the stability, prosperity, security and peace within nations and between and among nations. Its danger lies in its arbitrary destructiveness as much as in its unpredictability, and the constant threat of terrorist activity compels measures and actions that cause strain and contention in free, democratic societies as security concerns and civil liberty concerns must be balanced so that both public safety and civil liberties are maintained. Safety and security concerns can be addressed through numerous proactive steps and measures, many of which cause only minimal interference with and disruption of the daily routines of work, travel, commerce and entertainment. However, because modern industrial societies afford almost limitless places, locations, and opportunities for terrorist activities, no safety measure or security protocol will be foolproof, but many security measures, systems and protocols can be implemented that greatly minimize specific threats through fingerprint identification procedures, chemical, biological, and radiological hazard detections, bomb and explosive detection, and controlling the access to everything

from shipping containers to school lockers. Thus, the prior art discloses a wide range of security measures and systems.

For example, the Fishbine et al. patent (U.S. Pat. No. 4,792,226) discloses an optical fingerprinting system that includes an optics/processor unit, a video monitor, a data terminal, and a printer for collecting and storing data characteristics of all ten individual fingerprints for printing demographic information and fingerprint images as desired on a standard booking or applicant card.

The Schiller patent (U.S. Pat. No. 4,544,267) discloses a finger identification unit that includes a fingerprint scanning apparatus using a collimated beam of light to interrogate the fingerprint of a finger placed against a platen so that successive scan positions produce signals containing fingerprint information.

The Fishbine et al. patent (U.S. Pat. No. 5,222,152) discloses a portable fingerprint scanning apparatus for optically scanning and recording fingerprint images and wirelessly transmitting such images to a mobile processing unit for verification and background checking.

The Lougheed et al. patent (U.S. Pat. No. 5,233,404) discloses an optical scanning apparatus that uses a linear charge coupled device (CCD) for recording the image of a fingerprint on the viewing surface.

The Groger et al. patent (U.S. Pat. No. 5,766,956) discloses a diode laser based sensor for undertaking optical, chemical, immunological or nucleic acid-based assay or other chemical analysis.

The Feldman patent (U.S. Pat. No. 5,938,706) discloses a multi element security system for preventing the unauthorized use of an automotive vehicle, and which includes numerous locking and control features interconnected to an onboard cpu.

The Bowker et al. patent (U.S. Pat. No. 5,963,657) discloses a safety access control for doors, handles, locks, etc., wherein the surface relief of a finger is read and verified to either allow or prevent access by the individual to the door, handle, lock, etc.

The Bonder et al. patent (U.S. Pat. No. 6,078,265) discloses a fingerprint identification security system wherein a key lock operated security system utilizes the fingerprint of the individual to control user access to the security system, such as the ignition system of an automotive vehicle.

The Anzai et al. patent (U.S. Pat. No. 6,271,745 B1) discloses a keyless authorization system for use of a motor vehicle that includes fingerprint reading units located on the exterior or interior of the motor vehicle and which are coupled to a control unit for scanning, comparing and matching fingerprints to allow or disallow access to the motor vehicle.

The Hwang patent (U.S. Pat. No. 6,374,652 B1) discloses a fingerprint-activated doorknob in which a detecting sensor for a fingerprint is placed on the doorknob for measuring and searching the fingerprint against previously stored fingerprint inputs to control access to the door.

The Vor Keller et al. patent (U.S. Pat. No. 6,588,635 B2) discloses a safety holster for a firearm that includes a pivotally mounted retaining member and a fingerprint sensor for scanning fingerprint information so that only authorized users can withdraw the firearm from the holster.

The Corday et al. patent (U.S. Pat. No. 6,613,571 B2) discloses a method and system for detecting biological and chemical hazards in the mail that includes sensors placed within the mail box for sampling and testing ambient air and so that mail can be safely transported through the mail system.

The Nagata patent (U.S. Pat. No. 6,628,213 B2) discloses a coding method for digital signal coding and decoding that includes a CMI (code-marked inversion) method of signal coding.

Nonetheless, despite the ingenuity of the above devices, methods, and systems, there remains a need for a multi-detector and disabling lock system for use with various types of products collected together by common characteristics into product groupings for detecting chemical, biological and radiological agents and compounds and for selectively disabling and activating the product locks thereby preventing unauthorized entry and further contamination and preventing and thwarting terrorist activities.

SUMMARY OF THE INVENTION

The present invention comprehends a chemical/biological/radiological detector unit with a disabling locking system for protecting products that can be grouped into several product groupings, from terrorist activity, and also for preventing unauthorized access to and tampering with the storage and transport of ordnance and weapons. The products grouped into what may be referred to as Product grouping 1 include, but are not limited to, cargo containers, shipping containers, tractor trailers, mail carriers, mail boxes and lockers; while the products grouped into what may be referred to as Product grouping 2 include, but are not limited to, chemical, biological, radiological, and nuclear detectors, motion sensors and door sensors. The multi sensor detection system includes the capability to disable an existing lock or activate a lock located inside any of the products named in the product grouping categories upon activation of a sensor or detector included in the system. This is a significant feature for the multi sensor detection system as it prevents unauthorized, unequipped and untrained entry and access to the product thus preventing further contamination of the site and to individuals in the area.

The multi sensor detection and lock disabling system includes a detector case sized to fit in, upon or adjacent any of the aforedescribed products for detecting harmful and dangerous chemical, biological, and radiological agents, compounds and elements. In addition, the multi sensor detection and lock disabling system is capable of transmitting a signal to lock or disable a lock on the product, and is also capable of transmitting signals to a monitoring computer terminal or PC so that appropriate defensive and safeguarding actions can be undertaken and an authorized individual can disarm and reset the locking system and the multi sensor detection system. The detector case includes a power source (battery or electrical), interior compartments, Internet and GPS connections and a cpu interconnected with the Internet and GPS connections, and also interconnected with one or more off site monitoring computer terminals or PCs. The detector case includes one or more light alarm indicators that are externally visible and that light up when the chemical, biological, or radiological agent or compound is detected, and the light alarm indicators (which can be indicator lights or panels on the front of the detector case) can be color coded for denoting the specific agent or compound detected, i.e., separate and distinct colors for indicating detection of the chemical, biological, or radiological agent or compound.

The detector case is designed to hold within the interior compartments one or more interchangeable detectors, and each detector is adapted and set up to sample a specific compound or agent. Each detector includes a sound alarm, a sensor, a light alarm, and a readings panel, and is electrically interconnected (either by wire or wirelessly) to the cpu of the detector case so that information regarding the detection of the particular agent or compound can be conveyed from the detectors to the detector case cpu. Each detector can also be used as a manual, stand-alone hand held scanner.

The multi sensor detection and lock disabling system can be interconnected to a surveillance watchtower, as well as monitoring computer terminals or PCs, with the watchtower scanning shipping and cargo crates and containers being prepared for shipment or sitting for extended periods of time on a dock or at a port, at a railway site, or at an industrial storage facility. The watchtower will scan the cargo and shipping crates and containers for the light alarm indicators on detector cases that are mounted in or upon the crates and containers, and thus continuous security surveillance of the crates and containers can be maintained.

An enhanced version of the multi sensor detection and lock disabling system can be employed to prevent car and vehicle bombings. Coupling the multi sensor detection and lock disabling system with satellite service will enable the detection system to detect explosives and transmit an alert signal by satellite to monitoring equipment at a monitoring site. Upon receiving the alert signal at the monitoring site the monitoring equipment activates a stall-to-stop process for disabling the air, fuel, electrical and/or computer system of the vehicle. Moreover, upon receiving the alert signal at the monitoring site the car or vehicle will be locked by transmission of a satellite signal that disables the vehicle's electrical and ignition system thereby preventing escape of the terrorist.

It is an objective of the present invention to provide a multi sensor detection and disabling lock system for securing news racks and vending machines in order to prevent theft, unauthorized use and terrorist activity.

It is another objective of the present invention to provide a multi sensor detection and disabling lock system for preventing terrorist activity by using products grouped together by common features in several product groupings such as design similarity, similarity in the presentation of security problems and similarity with regard to the presentation of solutions to preventing terrorist solutions.

It is still yet another objective of the present invention to provide a multi sensor detection and disabling lock system that is capable of disabling an existing lock or activating a lock inside any of the products of the product grouping lists when a detector or sensor of the system is activated.

It is still yet a further objective of the present invention to provide a multi sensor detection and disabling lock system wherein the disabling lock system prevents the unauthorized entry, access and further contamination of the products included in the several product groupings.

A still further objective of the present invention is to provide a multi sensor detection and lock disabling system that utilizes a multi-task device for preventing terrorist activity to vulnerable products that are collected or arranged by product grouping categories.

Yet a further objective of the present invention is to provide a multi sensor detection and disabling lock system to secure cargos and containers, especially cargo and shipping containers, against chemical, biological, radiological and nuclear terrorist activity.

Still another objective of the present invention is to provide a multi sensor detection and disabling lock system capable of detecting chemical, biological and radiological agents and compounds.

Still yet another objective of the present invention is to provide a multi sensor detection and disabling lock system that includes interchangeable detectors that operate in conjunction to detect chemical, biological and radiological agents and compounds.

Still yet a further objective of the present invention is to provide a multi sensor detection and disabling lock system that can be implemented by business or government at a minimum cost by organizing the products to be protected into product grouping categories.

Another objective of the present invention is to provide a multi sensor detection and disabling lock system that accurately and reliably detects harmful agents, compounds and elements, and prevents the placement and storage of weapons and bombs in the range of storage containers and facilities currently available.

Still another objective of the present invention is to provide a multi sensor detection and disabling lock system wherein the interchangeable detectors that comprise part of the system can be used as stand-alone scanners.

These and other objects, features, and advantages will become apparent to those skilled in the art upon a perusal of the following detailed description read in conjunction with the accompanying drawing figures and appended claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the primary features of the system which include a detector case, several interchangeable detectors, an automatic/mechanical lock disabler and a fingerprint biometric lock with disabler;

FIG. **2** is a front elevational view of the multi sensor detection and lock disabling system of the present invention illustrating one of the interchangeable detectors first shown in FIG. **1**;

FIG. **3**a is a top plan view of the multi sensor detection and lock disabling system of the present invention illustrating the mounting of one lock disabler to the lock of a product, such as a container, and disengaged from the lock of the container,

FIG. **3**b is a top plan view of the multi sensor detection and lock disabling system of the present invention illustrating the engagement of the lock disabler to the lock of the product for locking or disabling the lock of the product so that unauthorized access is prevented;

FIG. **4** is a side elevational view of the multi sensor detection and lock disabling system of the present invention illustrating the detector case mounted to the product, such as the container, with the light alarm indicators externally visible;

FIG. **5** is a schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of detector cases with a surveillance watchtower and a monitoring PC terminal;

FIG. **6** is a schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the placement of detector cases upon containers different from the containers of FIG. **5**, and wherein the detectors case are interconnected to a surveillance watchtower and a monitoring PC terminal;

FIG. **7** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the mounting of one automatic/mechanical lock disabler to the lock of a standalone news rack;

FIG. **8** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating one interchangeable detector placed within the standalone news rack;

FIG. **9** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the detector case having color coded front panels for specifically indicating the agents, compounds or elements that have been detected;

FIG. **10** is a rear elevational view of the multi sensor detection and lock disabling system of the present invention illustrating the GPS, Internet and power source connections;

FIG. **11** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of the detector with the detector case and the steps undertaken by the system when an agent or compound is detected;

FIG. **12** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the sequence of steps undertaken by one detector when functioning as a stand alone scanner for detecting an agent or compound;

FIG. **13** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the interconnection of the detector case with the automatic/mechanical lock disabler for activating the lock disabler upon detection by the system of an agent or compound;

FIG. **14** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating interconnection of the detector case with the fingerprint biometric lock with disabler for engaging and disengaging the fingerprint biometric lock as part of the process of detection and safeguarding the public upon detection of the agent or compound;

FIG. **15** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of the system with a surveillance watchtower and a monitoring PC or computer terminal for monitoring containers, such as shipping or cargo containers, that may sit for extended time periods on docks, at rail yards, and at industrial storage facilities;

FIG. **16** is a representative schematic view of the multi sensor detection and lock disabling system of the present invention illustrating the integration of the detection system with a satellite and monitoring equipment at a monitoring site for detecting explosives placed in a vehicle and then transmitting signals to the satellite and then to the monitoring site for disabling and locking the vehicle;

FIG. **17** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of the features and elements of the detector case to a cell phone and cell phone case;

FIG. **18** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the incorporation of a GPS satellite, a monitoring site and a cell phone tower for communicating to and with an electronic device such as a laptop computer or a cell phone for transmitting signals to a vehicle for activating an onboard stall-to-stop device for bringing the vehicle to a halt; and

FIG. **19** is a perspective view of the multi sensor detection and lock disabling system of the present invention illustrating the use of a GPS satellite in conjunction with the monitoring site and monitoring equipment to relay commands and signals to the cpu or transceiver of the vehicle for stopping or locking the vehicle in response to a signal that a certain type of event (detection of a bomb, engine failure or malfunction or unauthorized use) has occurred or is in process.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Illustrated in FIGS. **1-19** is a multi sensor detection and lock disabling system **10** for preventing terrorist activity by

monitoring, detecting, and securing those critical areas, sites, and facilities vulnerable to terrorist activity. The first step is the identification of critical areas, sites, locations and facilities that are vulnerable to terrorist activity as convenient places to store and plant explosives and bombs and spread biological, chemical or radiological agents and compounds, followed by the disposition of the multi sensor detection and lock disabling system **10** for monitoring, detecting, and securing the particular location or site. Vulnerable sites, locations, facilities and areas are nearly limitless in their variety; in order to categorize the protection the present invention provides an anti-terrorist product grouping strategy has been developed wherein products made from the same or similar material, products having the same or similar design, and products presenting the same or similar security problems are grouped together with the multi sensor detection and lock disabling system **10** for preventing terrorist activity. For example, two preferred product groupings can be Product Grouping I: cargo containers, shipping containers, cargo planes, freight train cars, tractor trailers, mail carriers (UPS, FedEx), airport lockers, news racks (coin and non-coin operated), mail drop boxes, cluster mail boxes, keyed mail boxes, min-storage houses and buildings, bicycle lockers, stadium lockers, school lockers, cars, trucks, campers, buses, vans and utility vehicles. Product Grouping II: chemical detectors, biological detectors, radiological detectors, nuclear detectors, motion sensors, glass break sensors, plastic film on glass, high security locks, tampering labels, door sensors, disabling locking systems, vehicle detectors and satellite disabling locking systems. In addition to grouping products together by features, designs and materials, the multi sensor detection system **10** includes a lock disabling capability for disabling an existing lock or activating a lock on or inside any of the aforementioned products when a detector or sensor of the system is activated. The lock disabling feature is a crucial component of the invention in so far as it prevents unauthorized, unequipped or untrained individuals from gaining access and entry to the site and causing further contamination of the site.

As shown in FIGS. **1-10**, the multi sensor detection and lock disabling system **10** includes at least one—and preferably many—detector case **12** that can be placed in, on, upon or adjacent the product, such as the shipping containers **14** of FIGS. **4** and **5** resting upon a platform **16** or the cargo container **18** of FIG. **6** sitting upon a seaport dock or pier **20**. The detector case **12** includes a top **22**, a bottom **24**, a pair of opposed sides **26** and a front side or panel **28** and an opposite rear or back side **30**. The rear side **30** has connections or contacts that can include an Internet connection **32**, a GPS connection **34** and a power connection **36** for a power source. The power source for the detector system **10** can be any conventional battery or electrical source. The detector case **12** includes an interior chamber divided into a number of compartments **38** for holding therein agent or compound detection means hereinafter further described. A cpu **40** is mounted within the detector case **12** and electrically interconnects, routes, and transmits signals among items hereinafter further described and also communicates with a monitoring site and monitoring equipment. The front side **28** of the detector case **12** includes indicator means for visually indicating that a specific agent, compound or element has been detected. The indicator means can include color coded indicator lights **42** in panel form, as shown in FIG. **9**, with each indicator light panel **42** lighting up with a specific color corresponding to the detection of a specific agent or compound; or color coded indicator lights **44**, as shown FIG. **1**, that correspond to and individually light up on the detection of a specific agent or compound (chemical, biological, or radiological).

As shown in FIGS. **1**, **2** and **9-13**, the multi sensor detection and lock disabling system **10** includes a plurality of detectors **46** with each detector **46** adapted for and set up to sample for a specific agent or compound (biological, chemical, or radiological); and the detectors **46** are interchangeable for adapting to the needs and demands of future technology. The detectors **46** can also be used as stand alone scanners. In the preferred embodiment of the invention, at least three detectors **46** are placed within the detector case **12** with one detector **46** for specifically sampling biological agents or compounds, one detector **46** for sampling chemical agents or compounds, and one detector **46** for sampling radiological agents or compounds. The detectors **46** are interconnected to the cpu **40** of the detection system **10** by conventional connections that can be wire or wireless for transmitting the appropriate signals to the cpu **40** upon detection of the particular agent or compound. As shown in FIG. **2**, each detector **46** includes on its front plate or facing surface a sound alarm indicator **48**, a readings panel **50** comprising a plastic shield and LED lights for displaying the various read-out messages, a sensor **52** for detecting the specific agent, element or compound, and a light alarm indicator **54** that can be color coded for each specific agent and which is externally visible when the detector **46** is used as a stand alone scanner. Each detector **46** includes a conventional microprocessor for controlling the various functions and generating the appropriate signals for transmission to the cpu **40** of the detector case **12**.

As shown in FIGS. **1**, **3a**, **3b**, **9**, and **13-15**, used in conjunction with the multi sensor detection and lock disabling system **10** is at least one automatic/mechanical lock disabler **56**—and depending upon the number of products being monitored there can be one lock disabler **56** for each product. The automatic/mechanical lock disabler **56** is physically connected to the detector case **12** by a wire or cable **58** for receiving signals therefrom for disabling an existing lock or activating a lock inside a product to prevent access to the product. By way of example, FIG. **3a** shows the automatic/mechanical lock disabler **56** mounted—by any conventional means—to the lock **60** of the shipping container **14** shown in FIGS. **4** and **5** and connected by wire **58** to the cpu **40** of the detector case **12**. The lock disabler **56** is in the non-activated or disengaged state in FIG. **3a**. FIG. **3b** shows the automatic/mechanical lock disabler **56** mounted to the lock **60** of the shipping container **14** and in the activated or engaged state after detection of an agent or compound by the system **10** thereby for locking or disabling the lock **60** of the shipping container **14** and preventing unauthorized entry and access by unauthorized, untrained and unequipped individuals. In FIGS. **3a** and **3b** the lock **60** secures doors of the shipping container **14** that can be slidably or pivotably opened and closed.

In addition to the automatic/mechanical lock disabler **56**, the multi sensor detection and lock disabling system **10** can also utilize a fingerprint biometric lock with disabler **62** as shown in FIGS. **1** and **14**. The fingerprint biometric lock with disabler **62** is interconnected to the cpu **40** of the detector case **12** for receiving transmissions therefrom after detection of an agent or compound has occurred so that the lock on the product can be locked or disabled. Moreover, resetting of the fingerprint biometric lock with disabler **62** occurs when the fingerprint of the individual is placed on the fingerprint-matching pad **64**, and if a match occurs with a known fingerprint stored by the cpu **40**, then the individual can reset the fingerprint biometric lock with disabler **56** by turning the manual lock disabler **66**. The fingerprint biometric lock with

disabler **62** is mounted to the lock of the product in a manner similar to the mounting of the automatic/mechanical lock disabler **56** that is shown in FIGS. **3** and **3**b.

FIGS. **4** and **5** show one manner of disposition or placement of the detector case **12** in relation to the product, i.e., the shipping container **14**, with the color coded indicator lights **42** externally viewable; FIG. **5** shows a number of shipping containers **14** each equipped with a detector case **12** and integrated with elements hereinafter further described for continuously monitoring the shipping containers **14** as they sit for an extended period of time on the truck or rail platform **16**. FIG. **6** illustrates several cargo containers **18** sitting on the shipping dock or pier **20**, with each cargo container **18** having a detector case **12** mounted thereon and integrated with and monitored by elements shown in FIG. **5** and hereinafter further described.

FIG. **7** illustrates a typical product from product grouping **1** that is monitored by the multi sensor detection and lock disabling system **10** of the present invention; specifically, FIG. **7** shows a news rack **68** with one automatic/mechanical lock disabler **56** mounted to and interconnected with the locking mechanism of the news rack **68**. As long as there is no detection of any agent or compound, the lock disabler **56** is in the disengaged state, and the individual can deposit the coin amount in the chute and then freely open the glass panel **70** by the handle **72** for removing a paper. However, the lock disabler **56** would be activated upon detection of the harmful agent or compound and receipt of a signal from the cpu **40** for locking or disabling the locking mechanism thereby denying access to the interior of the news rack **68** from all untrained, unauthorized and unequipped individuals.

FIG. **8** illustrates one detector **46** disposed within the news rack **68** and which is visible through the panel **70** for detecting one specific agent, compound or element. The detector **46** functions as a stand-alone scanner and can be wirelessly interconnected to off site monitoring equipment.

FIG. **11** illustrates a representative schematic **74** for describing the signal transmission process from the detector **46** to the cpu **40** of the detector case **12**. The external stimulus **76** would be the chemical, biological or radiological agent or compound. If there is no detection of the agent or compound, the detector **46** will stay in the sensing mode **78**. However, detection of the specific agent will trigger the sound alarm **80** and the light alarm **82**, and instant transmittal of a signal to the cpu **40**. The readings **84** can be stored by the cpu **40** for verification and future review and evaluation. After all the appropriate corrective and preventative measures have been undertaken by the trained and authorized personal, and the site has been cleansed of the contamination, authorized and equipped personal can then reset **86** the system **10**.

FIG. **12** illustrates a representative schematic **88** for the detector **46** when used as stand-alone scanner. The detector **46** undergoes the same essential steps as illustrated in FIG. **11**, with the exception of the signal transmission to the cpu **40**. The detector **46** remains in detection mode **78** until an agent is detected, and then the various functions—light alarm **82**, sound alarm **80**, storage of readings **84**, and, after the appropriate security and safety steps have been carried out by authorized personal, detector reset **90** by authorized personal can occur thereby placing the detector **46** back in detection or sensing mode **78**.

FIG. **13** is a representative schematic **92** that illustrates the steps undertaken by the system **10** to lock or disable a lock, such as the lock **60** for the shipping container **14** shown in FIGS. **3**a and **3**b. Upon detection of the agent (chemical, biological, radiological) the alarm light indicators **42** or **44** will light up providing external indication that an agent has been detected. In addition, the system **10**—the cpu **40**—will transmit a lock/disable lock signal **94** to the automatic/mechanical lock disabler **56** to lock or disable the lock on the product, such as the lock **60** on the shipping container **14** of FIGS. **3**a-**5**. This prevents unauthorized, unequipped, or untrained individuals from entering or gaining access to the product for which a dangerous and perhaps lethal agent has been detected. After the proper authorities and authorized personal have been notified and all the appropriate security, preventative and clean up measures have been undertaken, the authorized individual can perform the disarm and reset function **96** for the system **10** placing the system **10** in back in the detection mode **98**.

FIG. **14** is a representative schematic **100** illustrating the use of the fingerprint biometric lock with disabler **62** with the system **10**. Upon detection of the agent or compound by the detector, the various alarms would sound and light up (shown in previous figures), and the cpu **40** would then transmit a signal to the fingerprint biometric lock with disabler **62** to lock or disable the lock on the product, such as the lock **60** on the shipping containers **14** shown in FIGS. **3**a-**5**. The shipping containers **60** would remain locked and in an access denied mode **101** should an attempt be made to gain access to the container **60** by opening the lock **60** with an unauthorized fingerprint. However, a fingerprint that matches stored and authorized fingerprints **102** would indicate an authorized individual, and would allow the individual to disable and disarm **104** the lock **60** of the shipping container **14**. The fingerprint biometric lock with disabler **62** would then be reset **106** after the appropriate safety, cleanup, and protection measures are completed, and the system **10** would be reset and placed back in the detection mode **108**.

FIG. **15** is a schematic representation **110** that illustrates the integration of a surveillance watchtower **112** and a monitoring terminal or PC **114** for monitoring products such as the shipping containers **14** or cargo containers **16** that sit for extended periods of time of docks, piers **20**, truck terminals, rail yards, shipping platforms **16** and industrial sites as shown in FIGS. **5** and **6**. The watchtower **112** would maintain continuous surveillance over a number of shipping containers **60**, for example, with detector cases **12** mounted in or on each container **14** and set in detection mode **116** with one or more detectors **46** disposed in each detector case **12**. The watchtower **112** would continuously scan for light alarm indicators **42** and **44** on the products, such as the containers **14** or **18**, and the watchtower **112** would be interconnected and integrated with the monitoring terminal or PC **114**. Upon detection **118** of an agent or compound in one or more of the shipping containers **14**, the appropriate light alarm indicators **42** or **44** would light providing visible confirmation of the detection of the specific agent or compound. The cpu **40** would transmit a lock/disable signal **120** to the lock **60** on each respective shipping container **14** to lock or disable the lock **60** thus preventing access to that respective shipping container **14**. In addition, signal transmissions would be sent to the monitoring terminal or PC **114** (which could be off site) thereby alerting authorized security personal of the contamination event. With the information received at the monitoring terminal **114**, authorized personal would then be notified and dispatched to the area to undertake the appropriate safety and cleanup measures **122**. Such measures would also include disarming the lock disabling system in order to gain access to the shipping container **14**. After all the cleanup and security measures are completed by the trained and properly equipped authorities, the detection system and the lock disabling feature would reset **124** and the detection system would again be placed in detection mode **116**.

FIG. **16** is a schematic representation **126** that illustrates an enhanced version of the multi sensor detection and lock disabling system **10** for preventing car and vehicle attacks and bombings. The lock disabling system **10** would be interconnected to the locking system and mechanism **128** of the vehicle **130**. In addition, a stall to stop disabling link **132** can be made with the fuel, air, and electrical system **134** of the vehicle **130**. The enhanced version incorporates a satellite **136** for signal receipt and transmission from the vehicle **130** in which the detector system **10** is placed to a monitoring site and monitoring equipment **138**. As shown in FIG. **16**, a detection signal **140** would be sent to the satellite **136** by the detection system **10** upon detection of a bomb or explosive **142** hidden in the vehicle **130**. The satellite **136** would then transmit an alert signal **144** to the monitoring site **138** with the signal **144** containing the relevant data to evaluate the nature of the threat. The monitoring site **138** would then transmit a stall to stop signal **146** to the detection system **10** to lock the vehicle **130** and/or disable the electrical system of the vehicle **130** thereby disabling the vehicle **130**, preventing access to the vehicle **130** by locking the vehicle **130**, and preventing any terrorist in the vehicle **130** from escaping.

The detector case **12** can be modified and adapted for inclusion with cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, suitcases, and briefcases. In addition, the basic monitoring terminal or PC **114**, as shown in FIGS. **5** and **15**, can be adapted and incorporated to include desktop PCs, notebook PCs, laptops, cell phones, LCD monitors, and satellite monitoring.

The system **10** and the watchtower **112**, along with the satellite **136** and the monitoring site **138** can be adapted or incorporated with cell phone towers and satellites for use with satellite communication and/or a cell tower, wi-fi, wi-max, broadband, GPS, navigation, radio frequency interconnected to a central processing unit (cpu), such as cpu **40**, or a transceiver and monitoring equipment to include but not to be limited to computers, laptops, notebooks, PC's, and cell phones for the receipt and transmission of signals therebetween. The aforementioned telecommunication and radio communication means can be interactive with any type of motive vehicle that includes but is not limited to cars, trucks, vans, SUVs, trains, subways, boats, ships and airplanes, and which is reported stolen, experiences a loss of brakes, or a bomb, explosives or other types of chemical, biological, radiological, or nuclear agents are detected within, upon, affixed or mounted to the vehicle and which detection causes an automatic signal transmission or a signal transmission is activated when a call is made to the monitoring station by an authorized person. The authorized individual includes but is not limited to the owner, pilot, conductor, captain, police highway patrol, security guard and military personnel to the monitoring equipment for activating a vehicle slowdown or stall-to-stop disabling system that similar to the disabling system **126** shown in FIG. **16**, or incorporating features of the system **126** shown in FIG. **16**, from the monitoring equipment to the vehicle. The activation of the stall-to-stop disabling means or the vehicle slowdown disables or engages the computer, electrical, fuel and air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to the brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and the horsepower of the motor.

In addition, the basic stall-to-stop disabling means or the vehicle slowdown means and device can be adapted, modified or designed to include: an open bust or open platform for integrating any new and innovative technology; warning lights indicators; sound alarm indicators; voice alarm indicators; a cell phone to transmit to the vehicle a signal for slowing and halting the vehicle; and a lock disabling system or means to lock a thief or terrorist inside the vehicle after a transmission is received or sent. Open bust or open platform also refers to the compatibility of the detector case **12**, or the incorporation of its features in cell phone cases, satellite cell phone cases, laptop cases, notebook PC cases, PDA cases, carry-on cases, briefcases, and suitcases, etc., with other communication, transmission and surveillance systems whereupon the detector case **12**, and its features, can be seamlessly integrated with other new and emerging systems and technologies.

Thus, as shown more specifically in FIG. **17**, by way of a representative example the features and elements of the detector case **12** are shown as being incorporated into cell phone detector case **150** and associated cell phone monitor **152**. The cell phone monitor **152** includes the standard keypad functions **154** and more specialized system use (ring tone, email, photos, texting) functions **156** as well as a viewing screen **158**. The cell phone detector case **150** includes a recharging cradle or seat **160**, a front side **162**, a top **164**, a bottom **166**, and a pair of opposed sides **168**. At the back of the cell phone detector case **150** are connections, contacts, and ports for at least an Internet connection **170**, a GPS connection **172**, and a contact, plug, or port for a power source **174**. The power source for the cell phone detector case **150** can be any conventional rechargeable battery source or standard electrical power from a standard electrical receptacle or outlet.

As shown in FIG. **17**, the cell phone detector case **150** includes one or more sensor/detector units, cells, or components **176** built into and incorporated into the case **150**. The detector **176** includes generally disposed at the front **162** of the case **150** the following types of indicators: a sound alarm indicator **178**, a readings panel **180**, a sensor **182** for detecting one or more specific types of agents, elements, chemicals, compounds, etc., and a light alarm indicator **184**. The sensor/detector **176** will be interconnected to the power source **174**. In addition, mounted on and externally visible on the sides **168** or front **162** of the case **150** are a plurality of color coded indicator lights **186** with each light **186** corresponding to a specific agent, element, chemical, compound, etc., and lighting up when that agent is detected by the sensor/detector **176**. The color coded indicator lights **186** will be electrically interconnected to the sensor/detectors **176** via any standard microprocessor. The cell phone detector case **150** and cell phone monitor **152** thus comprise a hand-held, easily portable and transportable detection means that is both effective and unobtrusive in its disposition and use.

FIGS. **18** and **19** illustrate representative examples of the integration of portable electronic communication or telecommunication devices such as a cell phone **187a** and/or a laptop computer **187b** with the monitoring equipment **138** located at a predesignated monitoring site **188**, and operating in conjunction with either a satellite and/or a cell phone tower **190** to transmit and receive signals and commands among each other and to a vehicle **192**, such as a truck, as part of a stall-to-stop disabling system for slowing and stopping the vehicle **192** and locking a thief, terrorist, or unauthorized individual in the vehicle **192** if needed. A wide range of events can trigger and initiate the stall-to-stop system and the locking or lock disabling system and mechanism, and the event doesn't have to be limited to the detection of a bomb or a chemical, biological, or radiological agent, element, or compound. The events can include, but is not limited to, detection of an engine problem to engine failure to the unauthorized use (stealing) of the vehicle **192**. The vehicle **192** includes an

electromotive system **194** that comprises, among other components, an onboard computer(s), electrical, fuel and air systems, as well as brakes, ignition, steering, and transmission. Also integrated with and capable of communicating with the vehicle's **192** electromotive system **194** is a stall-to-stop system while a lock disabling mechanism **196** is able to engage and disengage or disable the vehicle's **192** locking mechanism **198** upon receipt of the appropriate commands via a lock disabling communication channel or link **200**. This link **200** can also accommodate the stall-to-stop system commands and signals, and thus is a multi-channel communication link. A CPU or a transceiver **202** is programmed to receive signals from the cell phone tower **190** and/or to a GPS satellite **204** and is interconnected with the stall-to-stop system and the lock disabling system **196** via link **200** for engaging the electromotive system **194** and actuating the lock disabling system **196** to stop the vehicle **192** and lock inside the vehicle **192** anyone such as a thief, terrorist or other unauthorized individual.

A representative example for stopping, disabling, and locking the vehicle **192** that utilizes the cell phone tower **190** wherein the activation and/or distress signal **206** originates from the cell phone **187**a or the laptop **187**b and such activation signal **206** travels to the cell phone tower **190** that is nearest the current location of the vehicle **192**. A signal **208** is then transmitted to the monitoring site **188** and specific monitoring equipment **138** that can also include but is not limited to cell phones, laptops, desktop PC's, notebook PC's and LCD monitors. The monitoring site **138** then communicates by signal **210** to the GPS satellite **204** that an original or activation signal has been received and then the GPS satellite **204** locates and communicates by multiplex signal **212** with the CPU or transceiver **202** on the vehicle **192** and exchanges information on the type of problem, situation, location, and vehicle speed. The monitoring equipment **138** then transmits a signal **214** to the cell phone tower **190** that communicates with the transceiver **202** and/or CPU of the vehicle **192** to initiate or execute any commands that will actuate the stall-to-stop disabling link **200** and lock disabling system **196** for bringing the vehicle **192** to a halt and actuating the vehicle's **192** locking mechanism **198** for locking the thief, terrorist, or other unauthorized person inside the vehicle **192** if needed.

FIG. **19** illustrates a representative example wherein the stall-to-stop system and the lock disabling system **196** are utilized in conjunction with the GPS satellite **204**. In FIG. **19** a signal has traveled to the satellites nearest the vehicle's **192** current location and then the signal **218** has traveled to the monitoring equipment **138** and monitoring site **188** which can include but is not limited to satellite cell phones, satellite monitors, cell phones, laptops, desktop PC's, notebook PC's, and LCD monitors. The GPS satellite **204** then locates and communicates with the CPU and/or transceiver **202** on the vehicle **192** via a multiplex (two-way) signal **220** in order to exchange information on such distress and danger event parameters as the specific problem situation, location, and vehicle speed. The monitoring equipment **138** then transmits a signal **222** back to the GPS satellite **204** that in turn communicates via another signal **224** with the CPU and/or transceiver **202** to execute any commands to the stall-to-stop system for executing the disengagement of the vehicle's **192** electromotive system **194** for bringing the vehicle **192** to a halt and for actuating the lock disabling system **196** to direct the lock disabling link **200** to actuate the locking mechanism **198** thereby locking the vehicle **192** and anyone inside the vehicle **192**.

While the invention has been shown and described in a preferred embodiment, it will be apparent to those skilled in the art that numerous alterations, modifications, and variations will possible and practicable without departing from the spirit and scope of the invention as set forth by the appended claims.

I claim:

1. A stall-to-stop **[**and lock disabling**]** *or vehicle slow-down* system for slowing and stopping a vehicle **[**and locking passengers inside the vehicle**]** wherein the vehicle includes a transceiver *carried by the vehicle, and* a stall-to-stop *or vehicle slow-down* system **[**and a lock disabling system**]** that are interconnected to the electromotive system **[**and the locking mechanism**]** of the vehicle, comprising:

monitoring equipment located at a determinate monitoring site *that is remote from the vehicle and that is free from contact with the vehicle*;

at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom;

at least one **[**GPS**]** satellite capable of sending signals to the monitoring equipment and receiving signals from the monitoring equipment;

[the GPS**]** *wherein the at least one* satellite *or the at least one cell phone tower is* capable of **[**two-way**]** signal communication with the transceiver on the vehicle; and

whereupon a distress signal *made due to unauthorized use of the vehicle or an uncontrollable vehicle in use* sent by a *mobile,* portable, *or fixed* communication device to the cell phone tower *or satellite* causes a signal to be sent to the monitoring equipment which then communicates **[**with the GPS satellite so that the GPS satellite can locate and communicate**]** with the transceiver on the vehicle regarding specifics of the distress event parameters so that the monitoring equipment **[**and**]** *can send a signal to* the cell phone tower **[**can exchange signals**]** *or satellite* whereby the cell phone tower *or satellite* transmits to the transceiver so that the transceiver can execute commands that actuate the stall-to-stop *or vehicle slow-down* system **[**and the lock disabling system for stopping the vehicle and locking the vehicle so that anyone inside the vehicle remains in the vehicle**]**, *wherein the communication device is remote from both the vehicle and the monitoring site and is free from contact with both the vehicle and the monitoring site.*

2. The stall-to-stop **[**and lock disabling**]** *or vehicle slow-down* system of claim **1** wherein the **[**portable**]** *mobile* communication device is a cell phone, *a smart phone or handheld for the activating or deactivating of the stall-to-stop system; capable of locking or unlocking the vehicle doors and/or starting the vehicle.*

3. The stall-to-stop **[**and lock disabling**]** *or vehicle slow-down* system of claim **[2]** *1* wherein the portable communication device is a laptop computer.

4. The stall-to-stop **[**and lock disabling**]** *or vehicle slow-down* system of claim **[3]** *1* wherein the vehicle is an **[**airplane**]** *automobile.*

5. The stall-to-stop **[**and lock disabling**]** *or vehicle slow-down* system of claim **[4]** *1* wherein the vehicle is a railway train *or airplane.*

6. The stall-to-stop **[**and lock disabling**]** *or vehicle slow-down* system of claim **[5]** *1* wherein the vehicle is a ship.

7. A stall-to-stop and lock disabling system for slowing and stopping a vehicle and locking passengers inside the vehicle wherein the vehicle includes a transceiver *carried by the vehicle,* a stall-to-stop system and a lock disabling system that are interconnected to the electromotive system and the locking mechanism of the vehicle, comprising:

monitoring equipment located at a determinate monitoring site *that is remote from the vehicle and that is free from contact with the vehicle*;

at least one [GPS] satellite *or at least one cell phone tower* capable of sending and receiving signals to and from the monitoring equipment and the transceiver of the vehicle[;] *such that the*

[the GPS] *at least one* satellite *or at least one cell phone tower* capable of two-way signal communication with the transceiver of the vehicle; and

whereupon a distress signal *made due to unauthorized use of the vehicle* sent from a *mobile,* portable, *or fixed* telecommunication device to [the GPS] *a cell phone tower or a* satellite causes a signal to be sent to the monitoring equipment [followed by the GPS satellite locating and communicating with the transceiver of the vehicle] for exchanging information on the problem situation, location, and speed of the vehicle resulting in the monitoring equipment transmitting a signal to [the GPS] *a cell phone tower or a* satellite [and the GPS satellite] *for* communicating with the transceiver of the vehicle for executing commands that actuate the stall-to-stop system and the lock disabling system for stopping the vehicle and locking the vehicle so that anyone inside the vehicle must remain inside the vehicle *or locking the vehicle ignition to prevent the restarting of the vehicle;*

wherein the telecommunication device is remote from both the vehicle and the monitoring site and is free from contact with both the vehicle and the monitoring site.

8. The stall-to-stop and lock disabling system of claim **7** wherein the [portable] *mobile* communication device is a cell phone, *a smart phone or handheld for the activating or deactivating of the stall-to-stop system; capable of locking or unlocking the vehicle doors and/or starting the vehicle.*

9. The stall-to-stop and lock disabling system of claim [**8**] *7* wherein the portable communication device is a laptop computer.

10. The stall-to-stop and lock disabling system of claim [**9**] *7* wherein the [portable] *fixed* communication device is a [desktop PC] *telephone.*

11. A vehicle adapted for receipt of a signal from a remote location to control the vehicle's stall-to-stop means or vehicle slowdown means, comprising:

at least one of a brake, a foot peddle, a radar, a camera, a navigational system, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor;

an electrical system in electrical communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

a computer system in signal transmission communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

a receiver in electrical communication with the electrical system and adapted to receive at least one control signal from a remote location to activate a stall-to-stop means or vehicle slowdown means to stall or slow down the vehicle;

a receiver in computer communication with the computer system and adapted to receive at least one control signal from a remote location to activate a stall-to-stop means or vehicle slowdown means to stall or slow down the vehicle; and

wherein the at least one control signal is communicated from the receiver to the electrical system or the computer system to control at least one of the brake, the foot peddle, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

wherein the at least one control signal is sent due to unauthorized use of the vehicle, and wherein an originating first signal that eventually causes the at least one control signal to be sent is generated upon initial verification of the unauthorized use of the vehicle;

at least one mobile, portable, or fixed device capable of sending the at least one control signal from the remote location that is of electromagnet pulse, electrostatic discharge, microwave beam or radio frequency, to disable the computer, electrical, fuel and air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to the brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and horsepower of the motor.

12. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 11, further including a global positioning system (GPS) receiver adapted for communication with at least one satellite.

13. The stall-to-stop disabling and slowdown system of claim 11 wherein the stall-to-stop and slowdown means can be activated by an authorized individual which includes but is not limited to the owner, pilot, conductor, captain, police, highway patrol, security guard, port security and military personnel to the monitoring equipment from a fixed, portable or mobile communication device for activating the system.

14. The stall-to-stop disabling and slowdown system of claim 11 wherein a communication device; that of a cell phone, smart phone or handheld; capable of sending signals to the vehicle's operating equipment systems of at least one of, but not limited to, an ignition for starting and stopping, a lock for unlocking and locking, a horn for sounding; capable of receiving data and diagnostic information of the vehicle's operating equipment systems.

15. The stall-to-stop disabling and slowdown system of claim 11 wherein the disabling and slowdown means activation engages the computer, electrical, fuel, and/or air systems of the vehicle or a combination of the computer, electrical, fuel and air systems that include but are not limited to vehicle brakes, foot peddle, lights, speed controls, ignition, steering, transmission, and the horsepower of the motor.

16. The stall-to-stop disabling and slowdown system of claim 11 wherein the system can be adapted, modified or designed to include: an open bust or open platform for integrating any new and innovative technology that includes but is not limited to; warning lights indicators; sound alarm indicators; voice alarm indicators; a vehicle's electrical, mechanical or computer system for locking and unlocking of doors, windows, sun-roofs, trunks or hoods; applications for unlocking or locking a vehicle using a smart phone, cell phone or PDA.

17. The stall-to-stop disabling and slowdown system of claim 11 wherein the disabling and slowdown means reduces the speed of the vehicle to an idle speed and eventually stops the vehicle or to an advanced reduced stall and an immediate stop when the vehicle is in forward movement, backward or reverse movement, side movement, cruise control movement, or lane departure movement.

18. The stall-to-stop disabling and slowdown system of claim 11 wherein the disabling and slowdown means both have a flexible sequence of signals that includes a warning signal of flashing the vehicle lights or the locking of the doors can happened before or after the signal to stall-to-stop or signal to slowdown the vehicle is sent.

19. The stall-to-stop disabling and slowdown system of claim 11 wherein the disabling and slowdown means both have the ability to slowdown or stall the vehicle naturally and without any action on the brakes, door locks, or steering wheel, and both have the ability to slowdown or stall the vehicle through unnatural means where there may be action on the brakes, door locks, and steering for navigation to a safe stop.

20. The stall-to-stop disabling and slowdown system of claim 11 wherein the disabling and slowdown means including the devices that is monitoring, communication devices, communication equipment can be grouped into anti-terrorist product groupings based on the categories of similarities of design, of at least one of; sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices, vehicle slowing and stopping devices, specification, development and implementation; similarities in material composition of at least one of: steel, stainless steel, composites, brass, copper, aluminum, fiber, silicon, plastic, combining of materials parts or elements to form a whole; similarities in security problems of at least one of; theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.

21. The stall-to-stop disabling and slowdown system of claim 11 wherein the disabling and slowdown means is designed to be used with or without biometrics for authentication and identification, thereby allowing access to the product by authorized, trained and equipped individuals and preventing access to the products by unauthorized, untrained, and unequipped individuals.

22. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 11, wherein a communication link is present of at least one of a WiFi connection, a Broadband connection, an Internet connection, a Cellular connection, a Radio Frequency (RF) connection, a Bluetooth connection, and a Satellite connection, capable of signal communication thereto and therefrom monitoring equipment and a central processing unit (CPU) or a transceiver on the vehicle.

23. A vehicle adapted for receipt of a signal from a pre-programmed automated system to control the vehicles' stall-to-stop means or vehicle slowdown means, comprising:

at least one of a brake, a foot peddle, a radar, a camera, a navigational system, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor;

an electrical system in electrical communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

a computer system in signal transmission communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

a receiver in electrical communication with the electrical system and adapted to receive at least one control signal from a pre-programmed automated system to activate a stall-to-stop means or vehicle slowdown means to stall or slow down the vehicle;

a receiver in computer communication with the computer system and adapted to receive at least one control signal from a pre-programmed automated system to activate a stall-to-stop means or vehicle slowdown means to stall or slow down the vehicle; and

wherein the at least one control signal is communicated from the receiver to the electrical system or the computer system to control at least one of the brake, the foot peddle, the radar, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

wherein the receivers, the computer system, and the electrical system are part of at least one pre-programmed operating system of unintended acceleration, pre-crash, reverse acceleration, stabilization, lane departure, cruise control, driverless vehicle, and chemical biological radiological nuclear explosive (CBRNE) detection;

wherein the control signal to activate the stall-to-stop or vehicle slowdown is not remote from the vehicle and the signal to activate is initiated when at least one of the vehicle's operating systems for monitoring the vehicle's condition exceeds a pre-programmed vehicle operating system parameter.

24. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, further including a global positioning system (GPS) receiver adapted for communication with at least one satellite.

25. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, pre-programmed automated system further including a cellular communication device adapted for communication with at least one cell phone tower; further including, at least one satellite connection capable of communicating with the pre-programmed automated system; further including, at least one modem connection for short and long range radio frequency transmissions with the pre-programmed automated system.

26. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, where-in the at least one control signal is sent to the pre-programmed automated system for bringing a vehicle experiencing unintended acceleration to a slowdown, idle or stop.

27. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means when sensors of at least one of; navigation, camera, radar, guidance, motion, distance, weight, height are interconnected to the vehicles onboard electrical system and/or computer system for controlling at least one of a brake, a brake override system, an electronic throttle, a foot peddle, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor.

28. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means; when the vehicle is electric, a car, truck, ship, boat, train, or plane.

29. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means; when it is determined an emergency exist for the vehicle, driver, passenger(s), pedestrians or surrounding environment.

30. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means; when there is an in-vehicle notification warning of: crash, vehicle parking, speeding; driving too fast for conditions; construction zone; school zone; accident ahead; brake failure; acceleration/deceleration failure; acceleration/deceleration cruise control.

31. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means; when the vehicle is in forward movement, backward or reverse movement, side movement, cruise control movement, or lane departure movement or when the vehicle moves outside a designated perimeter or zone.

32. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, further includes vehicles pre-programmed to automatically activate the stall-to-stop means or vehicle slowdown means; when there is a detection of a bomb, weapon of mass destruction, chemical or biological agents, located in, on, or adjacent to a vehicle.

33. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, pre-programmed automated system is designed to be used with or without biometrics for authentication and identification, thereby allowing access to the vehicle by authorized, trained and equipped individuals and preventing access to the vehicle by unauthorized, untrained, and unequipped individuals.

34. The stall-to-stop disabling and slowdown system of claim 23 wherein the pre-programmed automated system can be grouped into anti-terrorist product groupings based on the categories of similarities of design, of at least one of; sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices, vehicle slowing and stopping devices, specification, development and implementation; similarities in material composition of at least one of: steel, stainless steel, composites, brass, copper, aluminum, fiber, silicon, plastic, combining of materials parts or elements to form a whole; similarities in security problems of at least one of; theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat; grouping security devices to form a network of ubiquitous sensing and detecting.

35. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 23, wherein a communication link is present of at least one of a WiFi connection, a Broadband connection, an Internet connection, a Cellular connection, a Radio Frequency (RF) connection, a Bluetooth connection, and a Satellite connection, capable of signal communication thereto and therefrom monitoring equipment and a central processing unit (CPU) or a transceiver on the vehicle.

36. Multi sensor detection, stall-to-stop, lock disabling system wherein the security systems can be grouped into anti-terrorist product groupings based on the categories of similarities of design of at least one of; sensors, software, interfaces, detector cases, locks, mobile communication devices, handheld communication devices, vehicle slowing and stopping devices, specification, development and implementation: similarities in material composition of at least one of; steel, stainless steel, composites, brass, copper, aluminum, fiber, silicon, plastic, combining of materials parts or elements to form a whole: similarities in security problems of at least one of; theft, detection for chemical, biological, radiological, nuclear, explosive compounds and agents, detection for weapons of mass destruction, biometrics for identifying terrorist, scanning to identify a terrorist threat, grouping security devices to form a network of ubiquitous sensing and detecting; comprising:

a multi sensor detection system with a plurality of interchangeable and integrable sensors detecting for chemical, biological, radiological, nuclear, explosive, human, contraband; camera, light and video sensors allow the user to access, review and respond to network multi sensor detection systems and view the environment from a cell phone, PDA, handheld, laptop, desktop, workstation or monitoring site;

a built-in, embedded multi sensor detection system for monitoring products with a plurality of interchangeable and integrable sensors detecting for chemical, biological, radiological, nuclear, explosive, human, contraband; camera, light and video sensors allow the user to access, review and respond to network multi sensor detection systems and view the environment from a cell phone, PDA, handheld, laptop, desktop, workstation or monitoring site; sensors for motion, locks, perimeter, temperature, tampering and breach for the prevention of terrorist activity and theft;

a cell phone; cell phone detection system with a plurality of interchangeable and integrable sensors detecting for chemical, biological, radiological, nuclear, explosive, contraband; camera, light and video sensors allow the user to access, review and respond to network cell phone detection systems and view the environment from a cell phone, PDA, handheld, laptop, desktop, workstation or monitoring site;

a stall-to-stop system with a stall to stop means and/or slowdown to idle means interconnected to a plurality of interchangeable and integrable sensors for speed, navigation, brakes, electrical, computer, air, fuel, motion, locks; camera, light and video sensors allow the user to access, review and respond to network stall-to-stop systems and view the environment from a cell phone, PDA, handheld, laptop, desktop, workstation or monitoring site;

an external automatic/mechanical lock disabler system with a plurality of interchangeable and integrable sensors detecting for chemical, biological, radiological, nuclear, explosive, contraband, perimeter, motion, tampering, temperature, breach; camera, light and video sensors allow the user to access, review and respond to network automatic/mechanical lock disabler systems and view the environment from a cell phone, PDA, handheld, laptop, desktop, workstation or monitoring site; capable of receiving and sending at least one signal of lock/unlock; wired or wireless; battery, solar or electrical; monitoring equipment and devices; communication equipment and devices; and/or biometrics to prevent entry or exit of unauthorized or untrained persons, thus locking any unauthorized or untrained persons, thief or terrorist inside any of the products listed in any of the product groupings categories; and

an internal automatic/mechanical lock disabler system with a plurality of interchangeable and integrable sensors detecting for chemical, biological, radiological, nuclear, explosive, contraband, human, perimeter, motion, tampering, temperature, breach; camera, light and video sensors allow the user to access, review and respond to network internal automatic/mechanical lock disabler systems and view the environment from a cell phone, PDA, handheld, laptop, desktop, workstation or monitoring site; capable of receiving and sending at

least one signal of lock/unlock; wired or wireless; battery, solar or electrical; monitoring equipment and devices; communication equipment and devices; and/or biometrics to prevent entry or exit of unauthorized or untrained persons, thus locking any unauthorized or untrained persons, thief or terrorist inside any of the products listed in any of the product groupings categories.

37. The internal automatic/mechanical lock disabler system of claim 36 is interconnected to the multi sensor detection system.

38. The internal automatic/mechanical lock disabler system of claim 36 is interconnected to the built-in multi sensor detection system.

39. The internal automatic/mechanical lock disabler system of claim 36 is interconnected to the cell phone; cell phone detection system.

40. The internal automatic/mechanical lock disabler system of claim 36 is interconnected to the stall-to-stop system.

41. The internal automatic/mechanical lock disabler system of claim 36 is interconnected to the external automatic/mechanical lock disabler system.

42. At least two of the security systems of claim 36; the multi sensor detection system; the built-in, embedded multi sensor detection system; the cell phone detection system; the stall-to-stop system; the external automatic/mechanical lock disabler system; the internal automatic/mechanical lock disabler system; the communication equipment, means and devices; the monitoring equipment, means and devices are operating independent of each other or interconnected with each other; capable of communicating therebetween; operating under at least one network and under at least one central control center.

43. Multi sensor detection, stall-to-stop, lock disabling system of claim 36, wherein a communication link is present of at least one of a WiFi connection, a Broadband connection, an Internet connection, a Cellular connection, a Radio Frequency (RF) connection, a Bluetooth connection, and a Satellite connection, capable of signal communication thereto and therefrom the monitoring equipment and a central processing unit (CPU) or a transceiver on the vehicle.

44. A vehicles' stall-to-stop system or vehicle slowdown system in signal communication with a pre-programmed automated system is adapted, modified, or designed to control the vehicles' stall-to-stop means or vehicle slowdown means, comprising:

an electrical system in electrical communication with at least one of a brake, a foot peddle, a radar, a camera, a navigational system, a light, a speed control, an ignition system, a steering wheel, a transmission, a fuel system, and a motor;

a computer system in signal transmission communication with at least one of the brake, the foot peddle, the radar, the camera, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor;

a receiver in electrical communication with the electrical system and adapted to receive at least one control signal from a pre-programmed automated system to activate a stall-to-stop means or vehicle slowdown means;

a receiver in computer communication with the computer system and adapted to receive at least one control signal in response to one of the vehicle's operating systems for monitoring the vehicle's condition upon exceeding a pre-programmed vehicle operating system parameter from the pre-programmed automated system to activate a stall-to-stop means or vehicle slowdown means such that the speed of the vehicle is initially decreased immediately after activation of the means upon initial receipt of the at least one control signal; and

wherein the at least one control signal is communicated from the receiver to the electrical system or the computer system to control at least one of the brake, the foot peddle, the radar, the navigational system, the light, the speed control, the ignition system, the steering wheel, the transmission, the fuel system, and the motor.

45. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 44, further can be adapted, modified or designed to include a global positioning system (GPS) receiver adapted for communication with at least one satellite.

46. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 44, further can be adapted, modified or designed to include a cellular communication device adapted for communication with at least one cell phone tower; further including, at least one satellite connection capable of communicating with the pre-programmed automated system; further including, at least one modem connection for short and long range radio frequency transmissions to and from the pre-programmed automated system.

47. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 44, further can be adapted, modified or designed to include a vehicle system designed to perform as a brake override system for stopping or slowing a vehicle experiencing unintended acceleration.

48. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 44, further can be adapted, modified or designed to include a vehicle system designed to perform as a pre-crash system for stopping or slowing a vehicle to prevent a crash.

49. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 44, further can be adapted, modified or designed to include a vehicle system designed to perform as a reverse acceleration slow-down system for stopping or slowing a vehicle traveling in reverse.

50. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 44, further can be adapted, modified or designed to include a vehicle system designed to perform as a stabilization system for stopping or slowing a vehicle to prevent a vehicle turnover.

51. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 44, further can be adapted, modified or designed to include a vehicle system designed to perform as a lane departure system for stopping or slowing a vehicle to prevent or minimize accidents when the vehicle begins to move out of its lane.

52. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 44, further can be adapted, modified or designed to include a vehicle system designed to perform as a remote vehicle slowdown system for stopping or slowing a vehicle by remote means.

53. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 44, further can be adapted, modified or designed to include a vehicle system designed to perform as an adjusted cruise control system for stopping or slowing a vehicle to prevent a crash.

54. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 44, further can be adapted, modified or designed to include a vehicle system designed to perform as a door lock and unlocking system for stopping or slowing the vehicle and locking a terrorist, thief, or user trying to elude the law inside the vehicle.

55. The vehicles' stall-to-stop means or the vehicles' slowdown means of claim 44, further can be adapted, modified or

designed to include a vehicle designed to perform as a driverless or autonomous vehicle for stopping or slowing a vehicle that is in operation with or without a user, driver or operator inside the vehicle.

56. The vehicles' stall-to-stop means or the vehicles' slow-down means of claim 44, further can be adapted, modified or designed to include a vehicle system designed to perform as a chemical, biological, radiological, nuclear and explosives detection system for stopping or slowing a vehicle when a harmful, hazardous, or dangerous compound or agent is detected.

57. The vehicles' stall-to-stop means or the vehicles' slow-down means of claim 44, wherein a communication link is present of at least one of a WiFi connection, a Broadband connection, an Internet connection, a Cellular connection, a Radio Frequency (RF) connection, a Bluetooth connection, and a Satellite connection, capable of signal communication thereto and therefrom monitoring equipment and a central processing unit (CPU) or a transceiver on the vehicle.

58. A stall-to-stop or vehicle slow-down system for slowing and stopping a vehicle wherein the vehicle includes a transceiver carried by the vehicle, and a stall-to-stop or vehicle slow-down system that are interconnected to the electromotive system of the vehicle, comprising:

at least one cell phone tower that sends a signal to the vehicle;

at least one satellite that sends a signal to the vehicle and receives a signal from the vehicle;

wherein the at least one satellite or the at least one cell phone tower is capable of signal communication with the transceiver on the vehicle; and

a communication device that is a cell phone, a smart phone, or a PDA that causes the signal to be sent from the cell phone tower to the vehicle that actuates the stall-to-stop or vehicle slow-down system due to unauthorized use of the vehicle, wherein the communication device is remote from the vehicle and free from contact with the vehicle.

59. The stall-to-stop or vehicle slow-down system of claim 58 wherein the at least one satellite or the at least one cell phone tower is capable of signal communication with the transceiver on the vehicle that is two-way signal communication.

60. The stall-to-stop or vehicle slow-down system of claim 58 wherein the communication device is a cell phone or a laptop computer.

61. The stall-to-stop or vehicle slow-down system of claim 58, further including a global positioning system (GPS) receiver adapted for communication with at least one satellite.

62. The stall-to-stop or vehicle slow-down system of claim 58, wherein a communication link is present of at least one of a WiFi connection, a Broadband connection, an Internet connection, a Cellular connection, a Radio Frequency (RF) connection, a Bluetooth connection, and a Satellite connection, capable of signal communication thereto and therefrom the monitoring equipment and a central processing unit (CPU) or the transceiver on the vehicle.

63. A stall-to-stop or vehicle slow-down system for slowing and stopping a vehicle wherein the vehicle includes a transceiver carried by the vehicle, and a stall-to-stop or vehicle slow-down system that are interconnected to the electromotive system of the vehicle, comprising:

monitoring equipment located at a determinate monitoring site that is remote from the vehicle and that is free from contact with the vehicle;

at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom;

at least one satellite capable of sending signals to the monitoring equipment and receiving signals from the monitoring equipment;

wherein the at least one satellite or the at least one cell phone tower is capable of signal communication with the transceiver or communication device on the vehicle; and

whereupon a distress signal made due to unauthorized use of the vehicle or an uncontrollable vehicle in use sent by a mobile, portable, or fixed communication device to the cell phone tower or satellite causes a signal to be sent to the monitoring equipment which then communicates with the transceiver on the vehicle regarding specifics of the distress event parameters so that the monitoring equipment can send a signal to the cell phone tower or satellite whereby the cell phone tower or satellite transmits to the transceiver so that the transceiver can execute commands that actuate the stall-to-stop or vehicle slow-down system,

wherein the communication device is remote the vehicle and is free from contact with the vehicle.

64. The stall-to-stop or vehicle slow-down system of claim 63 further including a global positioning system (GPS) receiver adapted for communication with at least one satellite.

65. The stall-to-stop or vehicle slow-down system of claim 63 wherein the at least one satellite or the at least one cell phone tower is capable of signal communication with the transceiver on the vehicle that is two-way signal communication.

66. The stall-to-stop or vehicle slow-down system of claim 63 wherein the specifics of the distress event parameters is the location of the vehicle.

67. The stall-to-stop or vehicle slow-down system of claim 63 wherein the distress signal is made by an owner of the vehicle.

68. The stall-to-stop or vehicle slow-down system of claim 63 wherein the distress signal is made by police.

69. The stall-to-stop or vehicle slow-down system of claim 63 wherein the monitoring equipment communicates automatically with the transceiver upon receipt of the signal caused by the distress signal.

70. The stall-to-stop or vehicle slow-down system of claim 63 wherein the distress signal is a signal that gives the location of the vehicle.

71. The stall-to-stop or vehicle slow-down system of claim 63 wherein the distress signal is a signal that gives information on the identity of the user of the vehicle.

72. The stall-to-stop or vehicle slow-down system of claim 63, wherein a communication link is present of at least one of a WiFi connection, a Broadband connection, an Internet connection, a Cellular connection, a Radio Frequency (RF) connection, a Bluetooth connection, and a Satellite connection, capable of signal communication thereto and therefrom the monitoring equipment and a central processing unit (CPU) or the transceiver on the vehicle.

73. A stall-to-stop and lock disabling system for slowing and stopping a vehicle and locking passengers inside the vehicle wherein the vehicle includes a transceiver carried by the vehicle, a stall-to-stop system and a lock disabling system that are interconnected to the electromotive system and the locking mechanism of the vehicle, comprising:

monitoring equipment located at a determinate monitoring site that is remote from the vehicle and that is free from contact with the vehicle;

at least one satellite or at least one cell phone tower capable of sending and receiving signals to and from the monitoring equipment and the transceiver of the vehicle such that the

at least one satellite or at least one cell phone tower capable of two-way signal communication with the transceiver of the vehicle; and

whereupon a distress signal made due to unauthorized use of the vehicle sent from a mobile, portable, or fixed communication device to a cell phone tower or a satellite causes a signal to be sent to the monitoring equipment for exchanging information on the problem situation, location, and speed of the vehicle resulting in the monitoring equipment transmitting a signal to a cell phone tower or a satellite for communicating with the transceiver of the vehicle for executing commands that actuate the stall-to-stop system and the lock disabling system for stopping the vehicle and locking the vehicle so that anyone inside the vehicle must remain inside the vehicle or locking the vehicle ignition to prevent the restarting of the vehicle;

wherein the communication device is remote from the vehicle and is free from contact with the vehicle.

74. The stall-to-stop or vehicle slow-down and lock disabling system of claim 73, further including a global positioning system (GPS) receiver adapted for communication with at least one satellite.

75. The stall-to-stop and lock disabling system of claim 73, wherein a communication link is present of at least one of a WiFi connection, a Broadband connection, an Internet connection, a Cellular connection, a Radio Frequency (RF) connection, a Bluetooth connection, and a Satellite connection, capable of signal communication thereto and therefrom the monitoring equipment and a central processing unit (CPU) or transceiver on the vehicle.

* * * * *